FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1325219-0

Total Deleted Page(s) = 82
Page 104 ~ b6; b7C; b7D;
Page 107 ~ b6; b7C; b7D;
Page 109 ~ b6; b7C; b7D;
Page 111 ~ b6; b7C; b7D;
Page 112 ~ b6; b7C; b7D;
Page 117 ~ Duplicate;
Page 118 ~ Duplicate;
Page 140 ~ b3; b6; b7C; b7E;
Page 141 ~ b3; b6; b7C; b7E;
Page 142 ~ b3; b6; b7C; b7E;
Page 143 ~ b3; b6; b7C; b7E;
Page 144 ~ b3; b6; b7C; b7E;
Page 145 ~ b3; b6; b7C; b7E;
Page 146 ~ b3; b6; b7C; b7E;
Page 147 ~ b3; b6; b7C; b7E;
Page 148 ~ b3; b6; b7C; b7E;
Page 149 ~ b3; b6; b7C; b7E;
Page 151 ~ Duplicate;
Page 152 ~ Duplicate;
Page 153 ~ Duplicate;
Page 154 ~ Duplicate;
Page 164 ~ Duplicate;
Page 165 ~ Duplicate;
Page 166 ~ Duplicate;
Page 167 ~ Duplicate;
Page 168 ~ Duplicate;
Page 169 ~ Duplicate;
Page 170 ~ Duplicate;
Page 171 ~ Duplicate;
Page 177 ~ Duplicate;
Page 178 ~ Duplicate;
Page 179 ~ Duplicate;
Page 180 ~ Duplicate;
Page 187 ~ Duplicate;
Page 188 ~ Duplicate;
Page 189 ~ Duplicate;
Page 190 ~ Duplicate;
Page 199 ~ Duplicate;
Page 200 ~ Duplicate;
Page 201 ~ Duplicate;
Page 202 ~ Duplicate;
Page 207 ~ b6; b7C; b7E;
Page 209 ~ Duplicate;
Page 210 ~ Duplicate;
Page 211 ~ Duplicate;
Page 212 ~ Duplicate;
Page 214 ~ Duplicate;
Page 216 ~ Duplicate;

Page 217 ~ Duplicate;
Page 218 ~ Duplicate;
Page 219 ~ Duplicate;
Page 221 ~ b6; b7C;
Page 222 ~ b6; b7C;
Page 247 ~ b6; b7C; b7D;
Page 249 ~ b6; b7C; b7D;
Page 250 ~ b6; b7C; b7D;
Page 251 ~ b6; b7C; b7D;
Page 252 ~ b6; b7C; b7D;
Page 253 ~ b6; b7C; b7D;
Page 254 ~ b6; b7C; b7D;
Page 255 ~ b6; b7C; b7D;
Page 257 ~ Duplicate;
Page 258 ~ Duplicate;
Page 259 ~ Duplicate;
Page 260 ~ Duplicate;
Page 261 ~ Duplicate;
Page 262 ~ Duplicate;
Page 263 ~ Duplicate;
Page 264 ~ Duplicate;
Page 265 ~ Duplicate;
Page 266 ~ Duplicate;
Page 274 ~ Duplicate;
Page 275 ~ Duplicate;
Page 276 ~ Duplicate;
Page 277 ~ Duplicate;
Page 278 ~ Duplicate;
Page 281 ~ Duplicate;
Page 282 ~ Duplicate;
Page 305 ~ Duplicate;
Page 306 ~ Duplicate;
Page 307 ~ Duplicate;
Page 308 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FD-272 (Rev. 3-3-59)

FEDERAL BUREAU OF INVESTIGATION

Reporting Office	Office of Origin	Date	Investigative Period
ALEXANDRIA	ALEXANDRIA	2/17/84	8/29/83 - 2/10/84

Title of Case	Report made by	Typed By:
MAINFRAME	SA [redacted]	gaj

Character of Case

FRAUD BY WIRE; CONSPIRACY

b6
b7C

PROSECUTIVE

REFERENCE: Alexandria teletype to the Bureau dated 8/27/83.

ADMINISTRATIVE:

This summary is organized into seven separate summaries to more clearly reflect the groups of subjects involved. Also, those summaries concerning juveniles were prepared separately in order to facilitate transmittal to local prosecutors.

Approved	Special Agent in Charge	Do not write in spaces below
		196-4713-30

Copies made:
2-Bureau (ICCOOJ CCRimDivn 2-23-84 jlm)
1-USA, Alexandria, Va.
(Attn: AUSA [redacted])
2-Alexandria (196A-633)

b6
b7C

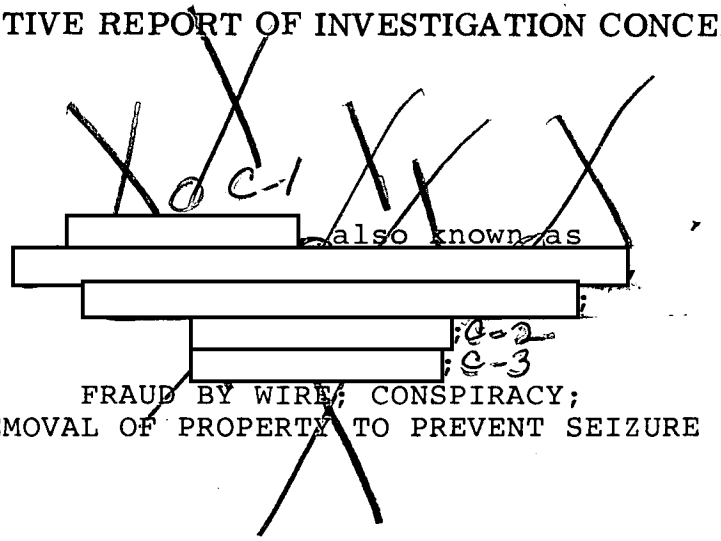
Notations:

A*
COVER PAGE

FD-517 (12-2-77)

FEDERAL BUREAU OF INVESTIGATION

PROSECUTIVE REPORT OF INVESTIGATION CONCERNING



b6
b7C

FRAUD BY WIRE; CONSPIRACY;
REMOVAL OF PROPERTY TO PREVENT SEIZURE

Copy to: 1 - USA, Alexandria, Va.
(Attn: AUSA)

b6
b7C

A 2

FBI/DOJ

AX 196A-633

TABLE OF CONTENTS

FD-518 (12-2-77)

Report of: SA [redacted] Office: Alexandria, Virginia b6 b7C
Date: 2/17/84

Field Office File #: 196A-633 Bureau File #:

Narrative of Offense:

General Telephone and Electronics (GTE) owns and operates a computer network known as Telenet which links various subscriber companies and Government agencies through a tie-in system in numerous cities throughout the United States. Access is obtained by calling a published telephone number in various cities.

Within the Telenet System is a service called Telemail which offers a computerized message capability between Telemail customers and any Telemail subscriber company. Each Telemail subscriber is responsible for designating an "in house" administrator to oversee all administrative functions of the customer's Telemail service, including the assignment of passwords to gain access to the system and the subscriber company. The administrator for a new user company may set up various subdivisions and individual users in his own company as he sees fit.

In August, 1983, GTE discovered that the accounts of approximately 18 Telemail subscribers had been accessed by unauthorized intruders from different areas of the country. The intruders gained access to certain customers' Telemail subscribers accounts by determining password assigned to Telemail subscribers through a process called "hacking". By this process, the "hacker" chose a subscriber account, such as Raytheon, NASA, USDA, RADA Corporation, Coca Cola USA, 3M Corporation. The "hacker" then tried numerous successive passwords (e.g., each letter of the alphabet, or the administrator's first name, etc.) until the correct password was discovered. Many hackers programmed their home computer to systematically try passwords for hours at a time. Once the hacker had broken a customer's password, he entered the Telemail System as if he were the legitimate subscriber. He did this by calling a published Telenet dial-in number and then placing his telephone on his modem hookup. This modem hookup allowed him to type on his home computer keyboard and have the impulses sent through the telephone system into the Telenet computer

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FBI/DOJ

system. He then typed in the command "Mail" and entered the Telemail message system. At this point the computer prompted him with "User Name?". He then typed in the words (for example) ADMIN/NASA. The computer then prompted with "Password?" and he then typed in the password that he had discovered through hacking. At this point he was accepted by the system as a legitimate subscriber, and was able to perform many of the functions that the subscriber can perform, all of which would be charged to the legitimate subscriber. At this point some of the hackers created a pirate subdivision in the legitimate subscriber organization, such as ADMIN/inner circle/NASA and set up user names in that new "pirate" account. User names may be any compilation of letters and numbers, but are usually a first initial, period, then last name (i.e., [redacted]). The hacker, as administrator of his own subdivision, then set up passwords for all his users, notified them of their user name and password and they could now enter Telemail with their names and passwords. These users could now leave messages on the system to an individual in the group, to the pirate administrator or (because the computer believed they are legitimate) to any other user (legitimate or illegitimate) in the entire Telemail system.

b6
b7C

On October 13, 1983, immediately before FBI Agents began a search of the WUSB Radio Station, State University of New York at Stony Brook, Stony Brook, New York, [redacted] told [redacted] to go into that room and remove certain items from that room to prevent those items from being seized. [redacted] did remove certain items from the room.

b6
b7C

AX 196A-633

NAME OF DEFENDANTS:

1. [redacted] described as:

Race
Sex
Date of Birth
Social Security Account Number
Address

[redacted] yrs old

b6
b7C

AX 196A-633

2. [redacted], described as:

Race
Sex
Date of Birth
Social Security
Account Number
Address

[redacted] yrs old

[redacted]

b6
b7C

AX 196A-633

3. [redacted] described as:

Race
Sex
Date of Birth
Height
Hair
Eyes
Address

[redacted] yrs old

b6
b7C

AX 196A-633

PROSECUTIVE STATUS:

1. On August 30, 1983, the available facts in this matter were presented to Elsie Munsell, United States Attorney, Eastern District of Virginia, who advised she would consider prosecution in the matter.

2. On October 13, 1983, the premises located at [redacted], and WUSB Radio Station, State University of New York at Stony Brook, Stony Brook, New York, was searched pursuant to a duly authorized federal search warrant and various computer paraphenalia were seized. b6 b7C

AX 196A-633

WITNESSES:

1. [redacted]
GTE Telemail
8229 Boone Boulevard
Vienna, Virginia
Telephone [redacted]

b6
b7C

Can provide details of GTE Telemail operations, methods of detecting unauthorized users and procedures for obtaining print-outs of customer messages.

2. [redacted]
Special Agent
Federal Bureau of Investigation

b6
b7C

Can supply details of investigation.

3. [redacted]
Special Agent
Federal Bureau of Investigation, New York

b6
b7C

Can supply details concerning search of WUSB Radio Station, State University of New York at Stony Brook.

4. [redacted]
Special Agent
Federal Bureau of Investigation, New York

b6
b7C

Can supply details concerning search of [redacted].

5. [redacted]

b6
b7C

Can supply details of admissions made by [redacted] to him, as well as details about the extent of intrusion into GTE Telemail by [redacted] and others.

Full text in report section, pages 7 - 16, attached.

6. [redacted]

b6
b7C
b7D

7. [redacted]

Telephone [redacted]

b6
b7C

Can provide details of [redacted] use of telephones and computers at WUSB, as well as details concerning [redacted] and [redacted] involvement in removal of evidence prior to FBI search.

b6
b7C

Full text in report section, pages 17 - 18, attached.

AX 196A-633

EVIDENCE:

1. Summary of 57 messages placed on GTE Telemail by [redacted] (originals in possession of [redacted], GTE Telemail). b6 b7C

2. Copy of 302 concerning search with attached list of items seized.

3. List of items from WUSB Radio Station, State University of New York, relevant to Telemail (originals in possession of Alexandria FBI).

4. List of items from [redacted] relevant to Telemail (originals in possession of Alexandria FBI). b6 b7C

5. List of charges for [redacted] and [redacted] (original in possession of [redacted]).

6. Copy of messages sent to GTE Telemail [redacted] (originals in possession of [redacted]). b6 b7C b7D

7. Copy of investigative reports provided by [redacted], Attorney for State University of New York at Stony Brook, concerning [redacted]. b6 b7C

8. Copy of letter from [redacted] with enclosed copy of "2600" magazine. b6 b7C

9. FD-302 summarizing trap and trace information received from [redacted]. b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/14/83

1

The following is a summary of messages left by the illegal user known as [redacted] and [redacted], on the GTE Telemail System. b6 b7C

The date and time of each message is provided, with a synoposis of particularly significant messages included.

1. July 9, 1983, 11:42 p.m. (All times Eastern Daylight Time) This message discusses a Source Account and states in part "Some of you mentioned hacking timecor and task force. What exactly are those and how are they accessible? I await your replies." Signed [redacted] b6 b7C

2. July 10, 1983, 4:28 a.m. Message reads as follows: "Hi, folks - [redacted] on assignment. The following will either be long and boring or informative and interesting, or maybe a combination. Looks like Southern Bell has some sort of relationship with Telenet." This is followed by a forwarded message from the Telenet Company that discusses "Southern Bell marketing opportunities for 1983/84." b6 b7C

3. July 14, 1983, 5:41 p.m This is again a forwarded message concerning the Telemail Account of Citibank.

4. July 15, 1983, 3:21 a.m. This is a forwarded message from [redacted] to all members of the Phalse group. The message is a listing of the projections of the 1984 Telemail Revenues. This message lists every current and projected Telemail account number and the projected revenue for 1984. b6 b7C

5. July 15, 1983, 3:25 a.m. This is another message from [redacted] to all members of the Phalse group, concerning Telenet information. b6 b7C

6. July 15, 1983, 11:27 p.m. This message discusses the idea of a publication called "2600 Magazine" with articles to discuss phone phreaking and computer hacking.

SOBE

Investigation on 12/8/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :pej Date dictated 12/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

7. July 10, 1983, 11:47 p.m.

8. July 11, 1983, 1:02 a.m.

9. July 16, 1983, 2:07 a.m. This message reads in part, "Yes, I have been thinking about distribution. So far we have reliable boxes in Colorado, Chicago and Long Island. I'm looking for a way right now of opening up a box in Grand Central Station or something." This message goes on to discuss ways that mail would immediately be forwarded to a different post office box so that the boxes could not be traced.

10. July 18, 1983, 3:02 p.m. This message states, [redacted] is the ID for the space station information." Signed [redacted] b6 b7C

11. July 18, 1983, 8:10 p.m.

12. July 18, 1983, 10:47 p.m. This is a message from [redacted] to [redacted]. The message begins, [redacted] (from [redacted])" and continues, "Give thanx, that you're not wanted dred (Sic) or alive. I'll be jammin with you tomorrow. Time to draw my brakes. What a plot! Police and thieves on my back. I gotta go back home to my tenament yard. [redacted] b6 b7C

13. July 24, 1983, 11:16 p.m. This message states, "I found this somewhere, but can't seem to get the procedure right. Any suggestions?" This is followed by the listing of a Telemail customer, computer application services and passwords for that customer.

14. July 25, 1983, 2:38 a.m.

15. August 2, 1983, 2:49 a.m. This message is entitled, "Your Telenet Guide," and discusses administrative functions of the Telemail system.

16. August 3, 1983, 1:30 a.m.

17. August 4, 1983, 4:05 a.m.

18. August 5, 1983, 7:03 p.m. In this message [redacted] is asking [redacted], aka [redacted], what the price range is for printing stationery. In a previous message, [redacted] indicated that [redacted] worked in a print shop. b6 b7C

19. August 8, 1983, 2:11 a.m. This message refers to [redacted] and [redacted], "hacking up a storm" on "Black". Black was their pseudonym for an IBM voice message system they were illegally using.

b6
b7C

20. August 8, 1983, 10:13 p.m. This message reads as follows, "[redacted], but Phalse isn't known by anyone yet. Is it? This is really the only place I've seen mentioned of it, unless they have bugs on ADS (which I really doubt), there's no real record Phalse anywhere. I think perhaps we should change our name when hacking perhaps, but then again it's always possible that some faithful follower (Phalse groupies) will do things in our name (or we could say that, anyway!)"

21. August 17, 1983, 10:13 p.m.

22. August 21, 1983, 11:45 p.m. This message discusses, "Green, gold, and black." These are IBM voice message systems that these people were using illegally.

23. August 23, 1983, 9:48 p.m.

24. August 24, 1983, 11:34 p.m.

25. August 26, 1983, 4:45 p.m.

26. August 29, 1983, 4:17 p.m. This message is entitled, "Arpa" and states in part, "I was able to get inside their Centrex using that 800 number I told you about."

27. August 31, 1983, 12:43 a.m.

28. August 31, 1983, 4:08 p.m.

29. August 31, 1983, 11:20 p.m. The statement reads in part, "Hi, [redacted], Good to see you got onto the system alright. Welcome to the Phalse network. Our purpose is to exchange all kinds of info as quickly and efficiently as possible. This system is one of our resources. If you'd like to see some of the stuff we've been up to, look in EMLE. The PW is the same as yours when you logged in."

b6
b7C

30. September 8, 1983, 3:56 a.m.

31. September 8, 1983, 5:37 a.m. In this message, [redacted] forwards a message from a Telenet official to all Telenet users discussing unauthorized access to customer computer systems. b6 b7C

32. September 8, 1983, 10:15 a.m. This message reads as follows, "The situation at Telenet continues to be unsettled, as those of you on the 'A' System can see on the BBS. Therefore the the moratorium against hacking Telemail accounts has been extended until the end of September. At that time, we can continue with a vegence and introduce the new people into the ways of the 'usercode.'
A new Arpa update has been sent to those currently involved in the TAC HAC Project. We still do not have a date on password cutover, although the end of the year has hinted at for MILNET implementation. We still need guest accounts on MIT and SRI hosts, as well as a new FTP NOCS. Anyone with info on any of these should pass it on via the Arpa list.
And last but not least, another reminder not to take the Telemail Customer Survey they are touting on the BB. It is partly designed as a trap to validate authorized system users, and our unregistered area which stands out like a sore thumb should they take a closer look. Later, all." Signed, [redacted], and is followed by "P.S.: OSUNY Lives!" b6 b7C

33. September 11, 1983, 5:13 p.m.

34. September 11, 1983, 5:19 p.m. This message states, "Folks, should we risk sending to these people from our own accounts? Personally I'd feel better if we had accounts over in their area in case as a clampdown or something. Please let me know the facts." Signed, [redacted] b6 b7C

35. September 12, 1983, 8:00 p.m.

36. September 12, 1983, 11:51 p.m.

37. September 13, 1983, 5:26 p.m.

38. September 14, 1983, 11:30 p.m.

39. September 17, 1983, 2:06 a.m.

40. September 17, 1983, 9:36 p.m.

41. September 18, 1983, 10:05 p.m.

42. September 18, 1983, 10:05 p.m.

43. September 19, 1983, 2:03 a.m.

44. September 24, 1983, 8:34 p.m.

45. September 25, 1983, 8:51 p.m.

46. September 27, 1983, 5:54 p.m.

47. September 28, 1983, 11:21 p.m.

48. September 29, 1983, 8:29 p.m. This message is an exhortation by [redacted] for all members of the Phalse group to use the illegal systems more frequently to keep in contact with each other. b6 b7C

49. September 30, 1983, 5:23 p.m.

50. October 1, 1983, 3:22 a.m.

51. October 3, 1983, 12:05 p.m.

52. October 6, 1983, 12:13 a.m.

53. October 10, 1983, 1:42 a.m.

54. October 10, 1983, 7:05 p.m. This message is from [redacted] to [redacted] and states, "Can we talk via voice sometime soon? Leave me a MSG somewhere." b6 b7C

55. October 11, 1983, 1:11 p.m.

56. October 11, 1983, 11:56 p.m.

57. October 12, 1983, 12:13 a.m.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription
10/25/83

On October 13, 1983, at 11:55 AM, a search warrant was executed at room 240 of Student Union Building Number 37 at the State University of New York at Stony Brook, New York, by Special Agents (SA's) [redacted] and [redacted]. No pertinent property was found at this location. b6 b7C

[redacted] of WUSB, advised that there was personal computer equipment belonging to [redacted] in room 227 of the same building and that the telephones in room 227 were part of the same system as those in room 240. [redacted] indicated that he had control over room 227 and would allow access. He proceeded to give his written consent for the Special Agents of the Federal Bureau of Investigation (FBI) to enter room 227. b6 b7C

At 12:30 PM, Magistrate SHIRA A. SCHEINDLIN of the Eastern District of New York at Brooklyn, New York, was contacted telephonically by Special Agent [redacted] and advised of the change in room locations and of [redacted] consent. SCHEINDLIN proceeded to authorize a search of room 227. b6 b7C

At 12:35 PM a search of room 227 was begun and the search was terminated at 2:15 PM. The search and inventory of property taken were made in the presence of [redacted], a volunteer employee of WUSB and part time user of the computer system. b6 b7C

At the time of the search, the Special Agents observed that the computer system in room 227 was connected to the telephone system.

Attached is a copy of the inventory of the property taken from room 227.

rviewed on 10/13/83 at Stony Brook, New York File # BQ 196B-2942

A [redacted] PRO/ SA [redacted] Date Dictated 10/19/83
A [redacted] and [redacted] PRO/sfn b6 b7C

document contains neither recommendations nor conclusions of the FBI.
s the property of the FBI and is loaned to your agency; it and its
ents are not to be distributed outside your agency.

10-13-83

INVENTORY MADE IN THE PRESENCE OF

[redacted] - Room 937, BEC, FBI [illegible]

b6
b7C

INVENTORY OF MATERIALS TAKEN PURSUANT TO WARRANT

1 SMALL FLIP N' FILE HOLD DISKETTES

1 LARGE " " W/41 DISKETTES

1 ZENITH MINICHESTER DISK DRIVE (CCN 2)(Serial# 2-607 5037 MCIS' CONTENTS SEE STAFF SERGEANT [redacted] MODEL NOTES)

1 HEATHKIT FLOPPY DISK SYSTEMS

1 CHARACTRONIC (#5404-45)

1 SMARTMODEM (#5300-4000)

1 HEATHKIT COMPUTER (CKS/D) MODEL H11-2, SERIAL NO. 0X-4039)

1 DIABLO 630 (SERIAL #[illegible] W/ LARGE PRINTER)

1 ZENITH 89 A MICROCOMPUTER (5037 Serial #5037) W/ACCESSORIES

1 SIDE CRAFT [illegible]

1 [illegible]

1 [illegible]

1 [illegible]

1 [illegible]

1 BOX OF MISC PAPERS & PRINTOUTS

1 MODEL [illegible]

1 [illegible]

CERTIFICATION

I swear that this inventory is a true and detailed account of all the property taken by me on the above date.

F-8

Subscribed and sworn to, and returned before me this date

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/14/83

The following is a review of items seized in a court-authorized search of the WUSB Radio Station premises at the State University of New York at Stoneybrook on October 12&13 1983. The following items of relevance to this investigation were found:

1) A computer print-out labeled "Telemail System Command Manual," printed September 20, 1983. This print-out contains all Telemail System commands. This information would normally be obtainable only by a legitimate Telemail administrator.

2) This item is another copy of the "Telemail System Command Manual."

3) A computer print-out titled "CP/M Modem Program Version 7.4." This is a program that will automatically search for other computer numbers through the telephone system.

4) A computer print-out beginning "Welcome to My Data Base System." This print-out also contains the statement "Hello, [redacted]." b6 b7C

5) A print-out entitled "Free Access Computerized BBS Directory." Copyright by Peter J. Keller. This print-out also bears the address [redacted] Data Base System, care of Tower Systems, 196 Main Street, Lincoln Park, New Jersey 07035, followed by the words Modem: 201/694-7425. b6 b7C

6) A white envelope with the return address: [redacted]. This envelope is addressed to WUSB Radio Station, Attention: [redacted] b6 b7C

7) A print-out titled "Jerihug Computer Club Finances as of 6/10/82." This print-out contains a list of names and expenses.

8) A box of business cards labelled "Litel Systems, Incorporated, 285 Locust Drive, Rocky Point, New York." It also has the name [redacted] and the telephone number [redacted]. b6 b7C

Investigation on 11/10/83 at Alexandria, Virginia File # Alexandria 196A-633 Sub E

by SA [redacted] :kar Date dictated 11/14/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

9) A computer print-out listing numerous bulletin boards and telephone numbers.

10) A computer print-out of telephone numbers, including numerous Telenet access numbers and Arpanet access numbers. This print-out also includes a handwritten note: 914/725-4064, Osuny. It also bears the number 800/424-6000, followed by the words Telenet 800. This print-out also has a "Connect address" for the Source.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/14/83

The following is a review of items seized in a search of [redacted]; b6 b7C

1) A WUSB staff telephone directory, including the numbers for [redacted]; and [redacted]. b6 b7C

2) A yellow piece of paper with the words "[redacted] and/or [redacted]," and the area code 213 followed by other phone numbers. One of these numbers is area code [redacted]. b6 b7C

3) Photocopy of article entitled "Telecorder" with a typewritten note signed [redacted] was a member of the Phalsers who went by the user name [redacted]. b6 b7C

4) Telephone bill for the number [redacted], dated August 22, 1983, with toll charges.

5) White envelope with the number [redacted] on it. b6 b7C

6) 1982 personal pocket diary of [redacted].

7) A New York telephone brochure with numerous telephone numbers written on it.

8) Telephone bill for number [redacted], dated June 22, 1983. b6 b7C

9) Telephone bill for the number [redacted], dated April 22, 1983.

10) Telephone bill for above number, dated May 22, 1983.

11) Telephone bill for above number, dated February 22, 1983.

12) An orange 3 by 5 card with numerous names and addresses on it.

Investigation on 11/10/83 at Alexandria, Virginia File # Alexandria 196A-633 Sub E

by SA [redacted] :kar Date dictated 11/14/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

13) A computer print-out starting with "Dial Your Match Commands" and the words "TUC BBS," followed by a phone number.

14) A small scrap of yellow paper with the number [redacted] on it. b6 b7C

15) A white scrap of paper with the address [redacted]. (illegible), [redacted]. b6 b7C

16) A brown scrap of paper with the address [redacted]. b6 b7C

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 1/20/84

The "floppy discs" that were seized in search of the WUSB radio station at the State University of New York, Stony Brook, New York, were examined by [redacted], a computer programmer. [redacted] indicated that the discs appear to have no information on them pertaining to GTE Telemail.

b6
b7C

Investigation on 1/17/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 1/17/84

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS
[redacted]	AHSC	$62.29	July, August, September
	UAW	$31.00	September
[redacted]	Maraven	$16.00	August, September
	Telenet	$108.00	July, August
[redacted]	BMW	$0.29	September
		$127.58	
[redacted]	CBOT	$2.00	September
[redacted]	RADA	$1.00	September
		$3.00	
[redacted]	Maraven	$24.00	August
	Telenet	$325.00	July
	Telenet	$151.00	August

b6 b7C

b6 b7C

b6 b7C

Sub E [redacted]

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

USER	COMPANY	AMOUNT	MONTHS	
[redacted] (Continued)	BMW	$55.00	September	
	BMW	$40.00	August	
	Maraven	$1.00	September	
[redacted]	BMW	$4.00	September	b6 b7C
	BMW	$1.00	August	
[redacted]	Raytheon	$19.00	September	
[redacted]	Scannet	$2.00	September	
		$621.00		
[redacted]	Maraven	$0.17	August	
	Telenet	$144.00	July	
	Telenet	$59.00	August	
[redacted]	BMW	$11.00	September	b6 b7C
[redacted]	UAW	$5.00	September	
[redacted]	Scannet	$6.00	September	
		$225.17		
[redacted]	BMW	$3.00	September	
	BMW	$0.17	August	
	Maraven	$1.00	September	
	Maraven	$8.00	August	b6 b7C
[redacted]	Maraven	$132.00	July	
	Maraven	$37.00	August	
[redacted]	AHSC	$15.00	August	
		$196.17		

USER	COMPANY	AMOUNT	MONTHS	
[redacted]	AHSC	$0.55	September	b6 b7C
	Telenet	$92.00	July	
	Telenet	$21.00	August	
	AHSC	$6.00	August	
		$119.55		
[redacted]	AHSC	$64.00	August	b6 b7C
	AHSC	$10.00	September	
	Raytheon	$5.00	August	
	Raytheon	$7.00	September	
	RADA	$1.00	September	
		$87.00		
[redacted]	AHSC	$88.00	August	b6 b7C
[redacted]	CBOT	$6.57	September	
	RADA	$115.00	August, September	
	AHSC	$35.00	August, September	b6 b7C
	BMW	$20.00	September	
[redacted]	MMM	$3.00	September	
		$179.57		
[redacted]	CBOT	$86.00	September	
	RADA	$8.00	September	b6 b7C
[redacted]	MMM	$3.00	September	
		$97.00		

USER	COMPANY	AMOUNT	MONTHS	
[redacted]	CBOT	$103.00	September	
	RADA	$4.00	September	b6 b7C
[redacted]	MMM	$7.00	September	
		$114.00		
[redacted]	CBOT	$87.00	September	
	RADA	$18.52	August, September	
[redacted]	RADA	$0.76	September	b6 b7C
[redacted]	CBOT	$287.00	September	
		$393.28		
[redacted]	CBOT	$2.00	September	
	RADA	$3.00	September	
[redacted]	CBOT	$0.90	September	b6 b7C
	RADA	$0.12	September	
		$6.02		
[redacted]	AHSC	$27.00	August, September	b6 b7C
	MMM	$5.00	September	
	RADA	$2.00	September	
		$34.00		
[redacted]	RADA	$8.00	August, September	
	CBOT	$0.17	September	b6 b7C
[redacted]	MMM	$0.42	September	
		$8.59		

USER	COMPANY	AMOUNT	MONTHS	
[redacted]	Raytheon	$5.00	September	b6 b7C
	AHSC	$4.00	August, September	
		$9.00		
[redacted]	AHSC	$4.50	August, September	
	RADA	$0.12	September	b6 b7C
[redacted]	Raytheon	$1.00	September	
		$5.68		
[redacted]	Raytheon	$109.00	September	b6 b7C
[redacted]	Raytheon	$41.00	September	b6 b7C
[redacted]	Raytheon	$107.00	September	b6 b7C
[redacted]	Raytheon	$76.00	September	b6 b7C
[redacted]	CBOT	$0.29	September	b6 b7C
	RADA	$85.00	August, September	
		$85.29		

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE Telemail, forwarded copies of the attached Telemail messages. b6 b7C

Review of the messages indicates that contact with GTE Telemail was made by a group using the name "Phalse". The "Members of Phalse" soon stated they could be called [redacted], or [redacted]. This person then began using an intermediary to deliver the messages. [redacted] b6 b7C b7D

[redacted], as well as another confidential source, have confirmed [redacted] b6 b7C b7D

In the series of messages attached, [redacted] admits to frequent and pervasive intrusion into the Telemail system, and also admits to reading the internal messages of legitimate users of Telemail. (Specifically, AT & T Long Lines.) b6 b7C

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633 Sub E

by SA [redacted]:sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

AX 196A-633 - ATTACHMENT

Sub E

Posted: Mon Nov 7, 1988 9:00 AM EST Msg: LOID-1585-8088

From: [redacted]

To: [redacted] b6 b7C

CC: [redacted]

Subj: HACKER MSG

APPARENTLY, THERE IS AN ORGANIZATION SPONSORING SOME OF THE RECENT ACTIVITY BY UNAUTHORIZED USERS ON TELEMAIL. I RECEIVED THE FOLLOWING MESSAGE FROM ONE OF THEIR REPRESENTATIVES.

CLAUDIA

Forwarded Message:

Subj: [redacted] Nov 6, 1988 4:52 PM EST Urgent Msg: LOID-1571-7191

From: [redacted] b6 b7C

To:

CC:

Subj: TELEMAIL SECURITY

[redacted]

WE BELIEVE THAT ANY "ORGANIZATION" THAT HAS BEEN RATHER ACTIVE IN THE TELEMAIL SITUATION OVER THE PAST FEW MONTHS, WE WISH TO ESTABLISH A DIALOGUE WITH [redacted] REGARDING THE RECENT STATE OF AFFAIRS.

WE BELIEVE THAT ANY "ORGANIZATION" THAT HAS BEEN RATHER ACTIVE IN THE TELEMAIL SITUATION OVER THE PAST FEW MONTHS, WE WISH TO ESTABLISH A DIALOGUE WITH [redacted] REGARDING THE RECENT STATE OF AFFAIRS.

PHALSE IS A GROUP THAT BELIEVES IN THE POTENTIAL APPLICATIONS OF ASSORTED TECHNOLOGICAL INNOVATIONS (YES, THAT MEANS HACKING). WE ARE BY NO MEANS MALEVOLENT. THIS WILL WILL BE BORNE OUT IN ANY MORE YOU HEAR FROM ANY OF OUR MEMBERS. WE DID NOT DESTROY ANY INFORMATION NOR DID WE PREVENT AUTHORIZED PEOPLE FROM GAINING ACCESS TO THE SYSTEM. WE DID NOT WASTE DISK SPACE. UNLIKE MANY LEGITIMATE USERS.

WHAT WE DID DO WAS TAKE ADVANTAGE OF SOME RATHER ILL-KNITWITS. MANY OF THESE HOLES JUST BEG TO BE REMEDIED-THERE ARE PROBABLY SCORES OF OTHER HACKERS NIBBLING AWAY ALL THROUGHOUT THE SYSTEM. WE FEEL YOU HAVE GONE ABOUT THIS PROBLEM IN THE WRONG WAY. CONFISCATING LEGITIMATELY BOUGHT EQUIPMENT ONLY SERVES TO VICTIMIZE INNOCENT PEOPLE-MANY OF WHOM HAVE NO KNOWLEDGE OF THE TELEMAIL SYSTEM. THIS TACTIC CERTAINLY DOESN'T DISCOURAGE HACKERS! IT'S DOUBTFUL THAT ANYTHING WILL. AND IT DEFINITELY DOES NOT LOOK GOOD INT THE EYES OF THE PUBLIC.

NATURALLY WE CANNOT SPEAK FOR OTHER GROUPS OR INDIVIDUALS. AS REPRESENTITIVES OF PHALSE, WE FEEL THAT SOME OF OUR MEMBERS AREN'T BEING TREATED WITH FAIRNESS. WE'D LIKE A CHANCE TO DISCUSS THIS.

PLEASE DO NOT BLOCK ACCESS TO THIS ACCOUNT AS WE SINCERELY WANT TO ESTABLISH MEANINGFUL COMMUNICATION.

[redacted] b6 b7C

PHALSE

Action? PUR

Purged.

Action?

```
                    1588   %00000000000000003064   %000000, 000000, 000000, 00304
>%H1f89
                    8073   %00000000000000017611   %000000, 000000, 000000, 01761
>%H220f
                    8719   %00000000000000021017   %000000, 000000, 000000, 02101
>EOF!
:dumbmcb

Enter SMN or <CR> to stop: bgid=1588-8073,detail

SMN: BGID-1588-8073
Posted date: November  7, 1983   8:57 AM
Delivery Options: 0000000000000000

Field    Type   Offset   Length
-----    ----   ------   ------
From        1        0        9
To          1        9        8
Subj        1       30       24
MIDL        1       16       14
Body        1       54      454

From
3047 4F77  3039 1713                              * 0W 09  *

To
3130 3F4C  4E01 0A0D                              * 1?L N    *

Subj
5345 3A20  5445 4C45  4D41 494C  2053 2511        * SE: TELEMAIL SE *
5552 4954  5920 2121                              * UIT!  *

MIDL
000E 0100  8000 5442  4470 2176  0420             * .....VPID154    *

Body
4920 5749  4C40 2041  4520 4941  5950 5920  * I WILL BE HAPPY  *
544F 2049  5354 4142  4C49 5348  2041 2044  * TO ESTABLISH A D *
4941 4C4F  2057 4954  4820 594F  5520 2049  * IALOG WITH YOU. I *
4E20 5748  4154 4554  4553 2041  4153 4553  * N WHATEVER ASSIS *
2049 5320  4150 5051  4550 5220  4154 4553  *  IS APPROPRIATES *
0A43 4F4E  5349 4445  5249 4527  2059 4F55  * .CONSIDERING YOU *
5220 5345  4345 4E54  2041 2154  2045 4954  * R RECENT ACTIVIT *
4945 5320  4F4E 2047  5445 2054  4540 4F4E  * IES ON NTS TELEN *
4554 2753  2053 5953  5445 4D20  2050 524F  * ET'S SYSTEM, PRO *
5649 4445  4420 5448  4154 0D0A  594F 5520  * VIDED THAT..YOU  *
4341 4C40  204D 5920  4F46 4649  4345 2041  * CALL MY OFFICE A *
4E44 2049  4445 4E54  4946 5920  594F 5552  * ND IDENTIFY YOUR *
5345 4D56  4553 2E0D  0A0D 0A49  274D 2053  * SELVES.....I'M S *
5552 4520  594F 5520  4341 4E20  554E 4445  * URE YOU CAN UNDE *
5253 5441  4E44 204D  5920 5245  4D55 4854  * RSTAND MY RELUCT *
414E 4345  2054 4F20  4449 5343  5553 5320  * ANCE TO DISCUSS  *
4D41 5454  4552 5320  4F46 2053  5543 4820  * MATTERS OF SUCH  *
5345 4E53  4954 4956  4954 590D  0A57 4954  * SENSITIVITY..WIT *
4820 534F  4D45 4F4E  4520 4920  444F 4E27  * H SOMEONE I DON' *
5420 4B4E  4F57 2E20  2041 4E44  2049 4620  * T KNOW.  AND IF  *
594F 5552  204D 4F54  4956 4553  2041 5245  * YOUR MOTIVES ARE *
2054 5255  4C59 204E  4F4E 4D41  4C49 4349  *  TRULY NONMALICI *
4F55 5320  2049 200D  0A57 4F55  4C44 2045  * OUS, I ..WOULD E *
5850 4543  5420 5448  4154 2059  4F55 2057  * XPECT THAT YOU W *
494C 4C20  4841 5645  204E 4F20  5245 4D55  * ILL HAVE NO RELU *
4354 414E  4345 2054  4F20 434F  4D50 4C59  * CTANCE TO COMPLY *
```

```
2E0D 0A0D   0A43 4C41   5544 4941   2049 4F55   *  ...CLAUDIA HOU *
5354 4F4E   0D0A                               *  TON..          *

Enter SMN or <CR> to stop: xgid-1588-8719,detail

SMN: XGID-1588-8719
Posted date: November  7, 1988 @ 1:32 PM
Delivery Options: 0000000000000000

Field    Type   Offset   Length
-----    ----   ------   ------
From        1        0        8
To          1        8        8
CC          1       16       10
Subj        1       54        0
MIDL        1       26       28
Body        1       42      678

From
5454 5437   3030 3020                          *  TTT7100        *

To
4540 6564   650D 0A0D                          *  Email...       *

CC
5079 7269   6E63 650D   0A0D                   *  Principe...    *

Subj
4865 6C6C   6F20 2020                          *  Hello          *

MIDL
000E 0100   6000 5642   4430 3134   3432 0003  *  .....VB0142 ..  *
0100 4000   5454 5437   3030 3020               *  ..@.TTT7 7     *

Body
5468 6973   2069 6574   7465 7220   6973 2061  *  This letter is a  *
6E20 7265   706F 6E73   6520 746F   2079 6F75  *  n response to yu  *
7220 6D65   6D6F 2074   6F20 4948   6F75 7374  *  r memo to the Host*
6F45 1E20   2054 6865   206D 6169   6C62 6F78  *  on. The mailbox  *
2079 6F75   2061 7265   2075 7369   6E67 0D0A  *   you are using..  *
6973 2071   7569 7465   2069 6E20   6547 6167  *  is quite illegal  *
2028 6173   2079 6F75   2068 4E4F   7720 2029  *   (as you know).   *
686F 7765   7665 7220   4920 7265   616C 6977  *  nowever I realli  *
2077 6F75   6C64 206C   696B 6520   746F 2068  *   would like to h  *
6176 6520   610D 0A44   6961 6C6F   6775 6520  *  ave a..dialogue   *
7769 7468   2079 6F75   2E20 2054   6F20 7468  *  with you.  To th  *
6174 2065   6E64 2020   4920 6861   7665 2061  *  at end, I have a  *
206C 6567   616C 206D   6169 6C62   6F78 2073  *   legal mailbox s  *
6574 2075   7020 666F   7220 796F   750D 0A75  *  et up for you..u  *
6E64 6572   2074 6865   206E 616D   6520 2250  *  nder the name "P  *
6872 6965   6E64 3222   2E20 2054   6865 2070  *  hriend2".  The p  *
6173 7377   6F72 6420   666F 7220   7468 6520  *  assword for the   *
626F 7820   6973 2074   6865 2073   6967 6E2D  *  box is the sign-  *
6F66 6620   796F 750D   0A75 7365   6420 7768  *  off you..used wh  *
656E 2079   6F75 2063   6F6E 7461   6374 6564  *  en you contacted  *
204D 732E   2048 6F75   7374 6F6E   2E20 2042  *  [redacted]. B  *
6173 6564   2075 706F   6E20 796F   7572 206C  *  ased upon your l  *
6574 7465   7220 2069   7420 7365   656D 7320  *  etter, it seems   *
796F 750D   0A72 6570   7265 7365   6E74 2061  *  you..represent a  *
2067 726F   7570 2E20   2049 2064   6F6E 2774  *   group.  I don't  *
206D 696E   6420 7461   6C6B 696E   6720 746F  *   mind talking to  *
```

b6
b7C

```
6B65 2063   6172 6520   6F66 2064   6973 7365   * will let you..ta *
6D69 6E61   7469 6E67   2074 6865   2070 6173   * [redacted]inating the pas *
7377 6F72   6420 746F   2079 6F75   7220 6772   * sword to your gr *
6F75 7020   6D65 6D62   6572 732E   0D0A 0D0A   * oup members..... *
5261 7468   6572 2074   6861 6E20   6765 7420   * Rather than get  *
696E 746F   2074 6865   2064 6574   6169 6C73   * into the details *
206F 6620   796F 7572   206C 6574   7465 7220   *  of your letter  *
746F 2043   6C61 7564   6961 2020   4920 776F   * to [redacted] I wo *
756C 6420   7261 7468   6572 0D0A   7761 6974   * uld rather..wait *
2075 6E74   696C 2077   6520 6861   6E20 6465   *  until we can de *
7665 6C6F   7020 6120   6469 616C   6F67 7565   * velop a dialogue *
2E0D 0A0D   0A43 6F6F   6B69 6E67   2066 6F72   * .....Looking for *
7761 7264   2074 6F20   6865 6172   696E 6720   * ward to hearing  *
6672 6F6D   2079 6F75   2E0D 0A0D   0A50 6872   * from you.....Phr *
6173 6564   0D0A                              * ased..          *
```

b6
b7C

```
Enter BMN or CCRO to stop:
logoff
:07 NOV 1983, 16:44

909 162.86 DISCONNECTED 00 20 00:00:06:44 259 39

@c 909162

909 162 REJECTING 80 17

@c 909173

909 173 CONNECTED

User name? [redacted]
Password?

  Name or password invalid.

User name? [redacted]
Password?

Welcome to TELEMAIL!
Your last access was Monday, Nov  7, 1983   4:35 PM

CHECK these bulletin boards:
  TELENET

 No.  Delivered     From                  Subject                    Lines

   1 Nov  7 15:02 [redacted]              Equipment Pickup             4

Command? [redacted]

  User's catalog.

Command?  s all

  Nothing found in bulletin board.

Command?  s purged
```

Posted: Tue Nov 8, 1983 1:03 PM EST Msg: AGID-1589-2038

From:
To: [redacted]

b6
b7C

WE CAN NOT GET INTO THE ACCOUNT, PLEASE ADVISE.

PHALSE

Command:

Posted: Fri Nov 25, 1983 4:28 PM EST Msg: RGID-1591-3845

From: [redacted]/PH.PHRASES/ASSOCIATES b6 b7C

To:

Subj: communications

(Please excuse the delay in responding to you, however things have been rather hectic lately. We do hope you understand.)

Thank you for responding and for setting up a special account for us. Admittedly, it seems a bit strange to actually have a "legal" account on this system. We hope that all parties involved will make the most of this setup.

We would like you to be completely honest with us concerning this investigation. (We don't actually expect you to be, but we're taking a chance.) We will attempt to be as open and as honest as we possibly can regarding our activities on the system. But please don't expect us to reveal the identities of our every last member to you, the press, or the F.B.I. There has been entirely too much publicity concerning this incident, and we aren't especially eager to see more. The after effects have been rather disheartening -- to say the least. Many of our friends and associates are afraid to talk freely on their telephones, in their homes, to their friends, etc. This kind of paranoia is very hard for anyone to have to live with. While this may or may not evoke sympathy from any party, we feel it was important for you to know how this sort of thing is affecting our lives. We need to know just what the status is at present. It's been over a month now since events took their course and nobody has been able to say just what's going to happen or when. We find this to be very disconcerting. Believe it or not, the equipment that was seized was not being used primarily for the purpose of breaking into TELEMAIL or any other system. Such "extra-curricular" activities, for the most part, comprised at most five percent of a given individual's time at his or her keyboard. The other ninety-five percent was devoted to legitimate computer use.

Our members do not steal equipment, nor do they ever use any of their "illegitimate" knowledge for profit. No true hacker does: that would take them nothing more than a common criminal.

Our appeal is for the unfinished computer programs that are needed for someone's classes and jobs. We've heard reports of one person who was writing a novel through a word processor -- a person who had nothing at all to do with any of this matter -- and is now living in virtual suspended animation. There are many other such cases, but the point has been made.

TELEMAIL was not an end in itself to us. We simply used it because it was fast, efficient, and convenient (in fact, we feel it's a potential goldmine for individual computer owners as well as corporations). Again, we don't know what other people were actually doing. Whatever it was, though, it could certainly have been curtailed via a few small precautions on your part. We would be more than happy to advise you on these and on the workings of your system in general, however, we really must know if there is any chance of equipment being returned in the future.

Please advise and forward this to all interested parties.

Yours,
The members of PHALSE

F-25

Posted: Sun Nov 27, 1983 12:58 PM EST Urgent Msg: PGID-1591-3973

From: [redacted]/PH.PHRASES/ASSOCIATES b6
To: b7C
Subj: oops

We should have sent the main message as URGENT with a RECEIPT, however, we goofed. So this one will have the receipt. The following message is the urgent one.

Sent at the request of PHALSE by [redacted]. [Give my regards to [redacted] and [redacted]...])

b6
b7C

Yours,
[redacted] (member of PHALSE)

Posted: Sun Nov 27, 1983 1:41 PM PST Msg: UG[D-1591-99]
From: [redacted]/PH.PHRASES/ASSOCIATES b6
To: b7C
Subj: Internal memo

[Portal]
Greenberg.PNenninger
COMMUNICATION FROM HACKERS (PHALSE)

Hey.

We have received [illegible] communications via TELEMAIL with a group of hackers named "PHALSE". This group has been authorized to use a mailbox named [illegible]. We communicate with them through a mailbox named "PHALSE".

Somewhere in your mailbox are two letters. One (To: PHALSE) is the first letter received from the group through their new mailbox. The other letter is my draft response to them. No letter has not been sent. We have not defined at Telenet how the communications will be carried out (i.e. a committee response or an individual one). I await your advice.

Regards

Posted: Sun Nov 27, 1983 1:43 PM PST Msg: VG[D-1591-99]
From: [redacted]/PH.PHRASES/ASSOCIATES
To:
Subj: Initial response (draft) b6
b7C

[redacted]
My Draft Response to PHALSE

You request honesty in our communications. I am glad to offer it, especially if I can expect it from you. However, very little, if anything, can be said about any investigations. We will do nothing to jeopardize current or future investigations.

I don't know if TELEMAIL is a goldmine, as you suggest in your letter; but it is a business. As such, we expect the users of the system will only be those individuals authorized by Telenet. You mention that a few small precautions on our part could curtail unauthorized intrusions. Please comment further on this, as I suspect you are quite expert on the topic. You also point out the usefulness of the system to business and personal computer users. The current uses of the system by our customers are already

ite varied, but I would so appreciate your commen on this topic.

you call for the return of equipment, citing it is only used five percent of the time for unauthorized breaking and entering. First, how often do burglars' tools, guns and bombs have to be used before they are considered dangerous? Is there any difference between burglars' tools and computer equipment, when the equipment is used to break and enter into a private system? Second, I wonder how many individuals use their equipment primarily for hacking activities? The challenges of hacking are often found elsewhere when using a computer for more useful expressions of creativity, as I'm sure you are aware. Imagine what might have been accomplished if all of the time and ability spent on hacking had been channelled into something more constructive.

As far as innocent people suffering harm as a result of losing their equipment, I suggest that those individuals consult their attorney to see what can be arranged with the authorities. I am especially sympathetic where the material is needed by students for their coursework. I assure you that the people at Telenet wish harm to no one. We are proud of our TELENAL service, and of the people behind the service. We owe it to our customers to have no tolerance for unauthorized and illegal break-ins into the system.

The account you are now communicating on is [illegible] encouraged to use it. I suggest you change the password frequently and limit the password distribution. It really will be quite difficult to communicate if the account is used by too many people. Help me by advising me who you are. I don't necessarily need names and addresses, but assume it would be helpful if more than one person will be responding. I'll leave the form of the definition to you.

Sincerely,

[redacted]

b6
b7C

ommand?

Posted: Tue Nov 29, 1988 11:30 PM EST Msg: YGID-1591-7364
From: [redacted]PH.PHRASES/ASSOCIATES b6 b7C
To:
Subj: message #8

Dear [redacted](we would like a name too!),

If it makes you HAPPY, you can refer to me as Emanuel Goldstein. I can assure you that I speak for others that have been silenced.

One thing we need to ascertain is whether or not anyone else is [illegible] with you under our name. Our personal trainer has said that [illegible] is talking to you and saying [illegible] Let's hope not. (You should have received 3 messages on this [illegible] including this one and the two that were sent over the [illegible]

We are perusing over hardware trying to see this from [illegible] view. And we will help you figure out how to [illegible] den the access to users. But, as we've already [illegible] did was not wrong in our view. We found a flaw in a PA [illegible] it to build a trigger. All we wanted to do was [illegible] ourselves.

[illegible] and we are quite interested in [illegible] and collaborative [illegible] at "2600". Hopefully, the results of this [illegible] on things and we can all benefit.

We understand TELEMAIL is a business, [illegible] circus (no personal offense intended). You [illegible] so many others have made when they turned into giants. [illegible] of things. You folks lost control. Fortunately, things [illegible] outrageously out of hand. And you have perhaps [illegible] this. We don't particularly care about Telemail's security budget or your plans with Southern Bell and Manhattan [illegible] or the various scenarios in NASA's space station. [illegible] of that and more, but it didn't really [illegible] else had seen it, results could have been [illegible] would that have been? Not ours, certainly, but ours. [illegible] don't leave their front doors wide open at night. You [illegible] we did was come in out of the rain.

Attorneys are great for people who can afford them. We are not rich enough to even use your system, much less protect ourselves from it! But one thing we have been told is that there is such a thing as due process, and it has not yet surfaced here. The media is starting to ask questions about that and we're really at a loss as to what to tell them, except that perhaps an exceptional error has occurred.

[redacted] ; - Executive office of the President

P.S. Tell those guys over on EXDP not to use first names as passwords. // Ambassadors should know better, after all.

Posted: Tue Nov 29, 1988 11:52 PM EST Msg: AGID-1591-7364
From: [redacted]PH.PHRASES/ASSOCIATES b6 b7C
To:
Subj: PHALSErs

This is [redacted] Suggestion, try asking Manny (name taken from the novel 1984) who [redacted] was....

Sounds like the PHALSERs want to help! HA HA

Somehow, I get the feeling that B.HARDY really doesn't think that they did anything wrong.... (the old hacker rationale...)
I wish there was some way to get across to him that he was completely wrong in his (and his friends) behavior.... Oh well....

Looks like there were several gangs loose on here. I can define most of them.

1. The Cracker and his friends from Irvine, Ca.
2. [redacted] and company.
3. The lovers from upstate New York.
4. The Inner Circle

[redacted]

and others

5. PHALSE

Bob Hardy

[redacted]

and others

6. [redacted] and [redacted] (???)

b6
b7C

b6
b7C

It's that #2 overlaps with #3 and #4 and that #4 and #5 ... I see, where [redacted] fits in I don't know. Lets have "Mason" tap.

B.HARDY tells me that someone's lawyer reports that there is [illegible] else talking to the FBI and/or TELEMAIL. "Mason" makes reference to that in his letter. I hope we are not dealing with an internal leak here....

I would sure like some direction from you guys to assist me in ensuing further. I do a fair job just improvising but I sure don't want to foul up anything by accident. Hopefully, my efforts on your behalf are helping rather than hindering. I must say, there are times when I have to pinch myself to be sure I am not dreaming all this stuff!!! ha ha

It is interesting hearing all sorts of tidbits from B.HARDY about what went on inside TELEMAIL. Looks like you had quite a time of it! Whew! My concern is that the investigation will drag, and drag, and drag, etc. and any momentum that will help discourage future system hackers will be lost. My own belief is that punishment should be as swift and sure as possible while still being fair. The longer you make these poor hackers wait for some sort of indictment, the more p.o.ed they will get. Now the teenagers on the other hand will lose their fear and want to begin hacking all over again.... There needs to be some sort of national clearing house for dealing with computer fraud and telecommunications abuse that is funded by a consortium of all telephone companies and data communications carriers. The kind of abuse that I am daily in contact with is mind boggling. If it is any consolation, the trials and tribulations of TELEMAIL are nothing compared to what is still happening on other systems every day!

(Well I will get down off my soapbox and get back to work.... Sorry about the outburst, but I have to get some of load off my mind to keep my sanity in this incredible mess.)

Yours,

Command?

b6
b7C

Posted: Sun Dec 18, 1983 10:01 AM EST Msg: WGID-1594-3922
From: [redacted] /PH.PHRASES/ASSOCIATES
To: [redacted]
CC: [redacted]
Subj: External Communication

b6
b7C

The following memo from Phalse underscores the reason for our deployment of the recent security software in Telemail. Phalse was quite comfortable in their use of Telemail, including their use of Admin capabilities to set up their own accounts. They even policed the abuses of others to some extent, unaltruistically to avoid the inevitable discovery and limitation of abuse.

We are still left with abuses where:
- Admins have not discovered accounts that were created by the hackers,
- Hackers have taken over accounts no longer used by the legitimate user (changing the default "A" to their own password),
- The legitimate user has a simple password (such as his/her first name) and doesn't change the password.

For your information, we have software installed, but not activated, that requires all users to change their passwords on a regular basis (i.e., monthly). This [illegible]

MESSAGE FROM PHALSE
==================

Posted: Sat Dec 17, 1983 [illegible] EST Msg: [illegible]
From: [redacted]
To: [redacted]
Subj: Part 1

b6
b7C

For many hackers, the initial discovery of TELEMAIL's infamous "A" default password came by word of mouth. For others, it was discovered by accident. On some occasions, was actually revealed by TELEMAIL administrators who unwittingly sent messages to each other, not knowing they were being overheard.

In whatever way it was discovered, the fact remained: TELEMAIL had made a very serious blunder by establishing a standard default for so many customers. It simply was not realistic to expect each and every company to take the responsibility of changing them. One of these subscribers (NASA) sent urgent messages to its members imploring them to change their passwords. But it was too late. While NASA, by inevitably changing their passwords structure, had prevented *further* breakins, there was very little that could be done regarding intruders that had already settled down in seldom or never used accounts. What's more, such people actually followed NASA's advice and changed their password, thus closing off the account to the original owner, who they hoped,

would try once, fail to get in, mutter something unprintable about computers and their creators, and then go back to his typewriter.

Most of the TELEMAIL hackers did not do anything malicious. However, we did hear reports of some people who sent silly messages or tried to start fights among legitimate users. PHALSE people were especially concerned about this, since everyonee's "safety" on the system was being compromised. When the crackdown came as it undoubtedly would, all of the hackers would be deemed as bad as the very worst. And so it went.

Administrator accounts proved to be rather easy to obtain as well, either the same "A" default or some mathematical equation involving the user ID number (a special code beginning with a "*") would spell out the password. Naturally, we were very concerned when the above people began bragging about getting into these accounts. We knew they wouldn't take the proper precautions and would wind up (however unwittingly) causing damage. They were warned repeatedly not to play around where they might be noticed, and not to create names that would attract attention (P.PHREAK, H.ACKER, etc.). It was naive to think this advice would be followed to the letter, but at the moment, we didn't know what else we could do.

We are not trying to throw the blame to somebody else --, we made many mistakes ourselves which we will outline in later messages. What we are doing is showing where PHALSE stood in relation to everyone else, as we have perceived it. If you have any specific questions regarding what we have already talked about, please address them here. The next message (hopefully Sunday) will be a continuation of this one.

[redacted] b6 b7C

MESSAGE FROM AN INTERMEDIARY
==========

[redacted] b6 b7C b7D

...

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

MY RESPONSE
==========

Manny,

No questions yet. Please continue.

[redacted]

b6
b7C
b7D

[redacted]

[redacted]

[redacted]

b6
b7C
b7D

Action? FYI

[redacted]

Action?

Posted: Mon Dec 19, 1983 12:39 AM EST Msg: PGID-1594-4019
From: [redacted]/PH.PHRASES/ASSOCIATES
To: [redacted]
CC: [redacted]
Subj: External Communications

b6
b7C

Followings are the letters received, and my responses to, Phalse and [redacted]

PhALSE MESSAGE
==========

Posted: Sun Dec 18, 1983 9:10 PM EST Msg: LOII-1574-1919
From: [redacted]
To: [redacted]
Subj: Part 2

b6
b7C

Once a TELEMAIL account has been successfully penetrated, further access was made easy through the generosity of TELEMAIL itself in dispensing information.

The DIRECTORY command was the most useful. By typing DIR, followed by a user name, one would get information about the user, assuming the user name existed. Of course, it was a bit tedious trying to [illegible] with user names ourselves. We couldn't be too silly with the user names were. After a little experimenting, we found that DIR would give us every user name that had an "A" in it somewhere. That list had certainly been made. But it still wasn't enough. We wanted to see more things. It didn't take long to discover that DIR would give us just that (except for the private data, which we will get to). This huge list made it possible to do several things. Since each DIR readout gave a little hierarchy structure, we were able to see what companies or organizations were on the system. From there, it was easy to use the USERS OF or MEMBERS OF commands to sort out users by company.

We were curious as to how many of these companies we could penetrate. So we went down the list, trying "A", or a first name (also worked in most cases by the DIR command), or even the user name itself. Some companies were not penetrated by us (TYMNET, TELNET, GMAC). Others were absurdly easy (NASA, US Dept. of Agriculture, Coca-Cola, and we are sorry to say, TELENET).

Every time a new account was entered, more information was obtained. For example, let's say we just got into an account used by NASA. We could now do a USERS OF NASA and get more names than if we did it from another non-NASA account. The entire structure of TELEMAIL was, thus, becoming unraveled right before our eyes.

No matter where we ended up, though, there was always private data which we could not see. And it was easy to figure out how to get this, although not very practical. A special user ID code had been assigned to each user ID. It began with a "*" and was shown with every DIR readout. If, instead of the user ID, you entered the user ID code, the same information would be displayed. All that would have to be done to get a list of *everybody* would be to keep feeding out different user ID codes (either sequentially or randomly) after the DIR command. This was much easier than trying to guess names. A computer could do it willingly. But it still would have taken a very long time, if we had ever decided to really pursue this. We were never able to find out whether a wildcard format might work here (DIR *'A' or DIR *'').

In a future message, we will talk about what we were actually doing on the system. For now, though, we would like to point out that we look on this whole mission of discovery as an Adventure. We were more interested in seeing how many accounts *could* be obtained through various companies than we were in actually obtaining them. For one thing, there was no need for us to attain new accounts, since we had enough to communicate with already.

Our next subject will be our suggestions towards improving security in the TELEMAIL system. First, however, we would like to open it up to the floor for questions or comments on what we have gone over so far.

[redacted] b6 b7C

[redacted] b6 b7C b7D

[redacted] b7D

[redacted] b7D

[redacted] b6 b7C b7D

[redacted]

b6
b7C
b7D

[redacted]

b7D

[redacted]

b6
b7C
b7D

[redacted]

b7D

[redacted]

b6
b7C
b7D

[redacted]

[redacted]

[redacted]

b6
b7C
b7D

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

MY RESPONSE
==========

[redacted]

Response to Part III

b6
b7C

[redacted]

Thanks again for your input. The "Floor", as you suggest, has no relevance at this time. Naturally, we are very familiar with the functionality of the various commands of Telemail (i.e. DIR/USER:/MEMBER etc.).

However, I am interested in what your thoughts are as to prevention of abuse. Clearly, this is where we can most benefit our user community. Detection is, at best, reactionary. How do you think we can discourage "would" hackers in the beginning of their "adventure"? You also suggest that we will expound upon what you have accomplished on Telemail. Please do.

Please bear in mind that Telemail is only one of many [illegible] in the future, certainly in our estimation. [illegible] interest to all. [illegible] responses. Actually, I hope that [illegible] improve the usefulness and security [illegible].

[redacted]

[redacted]

b6
b7C

Response to [redacted]

I certainly hope you change your password frequently. Why are you so paranoid about dealing with someone named "Phriend"? I really am.

As far as contacting Bud to find out his name, if you know his [illegible] anyone. I will get an account for you this way.

[redacted]

b6
b7C

Action? PUR

Purged.

Action?

Posted: Wed Dec 21, 1988 1:53 PM EST Msg: VOID-[illegible]

From: [redacted] PH.PHRASES/ASSOCIATES

To: [redacted] b6
b7C

CC: [redacted]

Subj: External Communications

FYI.

Forwarded message:

[redacted] b6
b7C
b7D

[redacted] b7D

[redacted] b7D

[redacted] b6
b7C
b7D

Action? PUH

Pursed.

Action?

Posted: Sat Dec 24, 1988 9:57 PM EST Msg: SRIJI-1595-2590

From: [redacted]/PH.PHRASES/ASSOCIATES b6 b7C

To:

Subj: Sorry for delay.

We are rather busy here and will try to continue our narative next week when we can find the time. The Holidays are a busy time. We are sure you will understand. Later...

[redacted] b6 b7C

Command:

[redacted] $ SINCE 12/22/95 PURGED

User's catalog.

*** Next cmd: S'SINCE 12/22

Bulletin Board contains:

No	Delivered	From	Subject	Lines
1	Dec 26 21:38	[redacted]	RE: Sorry for delay.	

b6
b7C

*** Next cmd: S PURGED

Nothing found in bulletin board

Command: R1

Postmark: Mon, Dec 26, 1995 4:39 PM PST
From: [redacted]@PWGATES/PWGATES
To:
Subject: RE: Sorry for delay.

b6
b7C

I wanted to understand. Merry Christmas and a Happy New Year!

F-40

[redacted]

b6
b7C
b7D

[redacted]

b7D

[redacted]

b6
b7C
b7D

[redacted]

b7D

Sent: Sat, Dec 21, 1996 11:46 AM EST Urgent Re: Miscellaneous
From: [redacted] (PH, Public Affairs)
To:
Subj: Further Communications

Please read my e-mail to the system I just sent. Also, I have more information, if you need it. Please call me at my office. Thanks.

Mary

Sent: Sat, Dec 21, 1996 9:10 AM EST Re: Miscellaneous
From: [redacted] (PH, Public Affairs)
To:
CC:
Subj: Messages Inbound

b6
b7C

Following are listings of messages inbound/outbound for the Phoenix mailbox. If you would like, I can download the entire message text. Please advise.

INBOUND MESSAGES
================

No.	Delivered	From	Subject	Lines
1	Nov 7 16:04	[redacted]	Initial Phase message	40
2	Nov 25 16:28		communications	54
3	Nov 29 23:20		message #3	43
4	Dec 9 0:39		more communications	72
5	Dec 17 23:11		Part 1	43
6	Dec 19 21:19		Part 2	50
7	Dec 24 15:47		Sorry for delay,	5
8	Dec 31 0:45		Further communications	17

b6
b7C

OUTBOUND MESSAGES
=================

No.	Delivered	From	Subject	Lines
1	Nov 7 17:1	[redacted]	[illegible]	7
2	Nov 25 17:17		[illegible]	41
3	Dec 9 14:03		[illegible]	44
4	Dec 19 0:40		Pleasantness	4

b6
b7C

[redacted]

b6
b7C

Command?

Posted: Fri Jan 13, 1984 3:19 AM EST Mss: AGIE-1597-3738
From: [redacted]/PH.PHRASES/ASSOCIATES b6 b7C
To:
Subj: AN EXPLANATION

Hello,

As you've probably noticed, communications have deteriorated. This has not been intentional. Events hAve transpired to drastically cut back access to this system. Here is a brief explanation.

This is only the second time that I (Manny) have communicated with you directly. Before this, I would dictate my messages over the phone to someone with a terminal who would then send them to you.

Recently I discovered that this person was really an FBI informant. So, for a time, I wasn't sure whether or not the messages had been sent or even if the account existed. So for the past two weeks, I've been scrimping and saving to get ahold of a terminal. That accomplished, I can now resume communications.

There have been a lot of nasty side-effects caused by this latest revelation, however. For one thing, my REAL name and unlisted phone number are being thrown all over the country, which is a bit of a bother. It wouldn't surprise me at all if you already had them. It also wouldn't surprise me if you were actually part of the FBI yourself (or selves). These possibilities don't upset me, although I do appreciate honesty when discussing such things.

What does upset me, though, is the way in which this entire thing is going. Apart from the threatening calls I get on an almost daily basis, friends of mine are being harassed because they know me. I don't know if this is the usual FBI routine, but it seems a bit much for what we're talking about.

For some reason, PHALSE is considered by them to be some huge and dangerous organization. I don't know how they interpreted the messages they read, but from what I know, nothing could be further from the truth. PHALSE is actually more of a state of mind than an actual group, but I certainly don't want to bore you with my interpretation.

I would appreciate any suggestions or revealing statements you might have at this point. Also, from now on, I will be speaking primarily from my own point of view instead of claiming to represent the "group". To continue to do that might spread the wrong idea even further.

Again, thanks for sending the copies of the messages so readily. They were a great help. If I'm not mistaken, though, you're missing one after your outbound #3. I seem to recall a message that said something to the effect of "this has been the most constructive message so far." As long as you remember it, that's fine.

There are two more topics [at least] that I had planned to address (preventative measures for you & an explanation of what we were doing on the system). I'm hoping for later on today for at least one of those. Purpose of this message was to let you know EXACTLY what's happening on this end and to try and explain the spottiness of our communications. Hopefully, I'll be able to finish these messages before I get an invitation to Alexandria, which I'm told could come at any moment.

Looking forward to your reply,

Manny

P.S. I'm using 800-424-9494. Is that OK?

P.P.S. Did you get "2600" yet?

Posted: Fri Jan 13, 1984 1:41 PM EST Msg: JGIE-1597-4709
From: [redacted]PH.PHRASES/ASSOCIATES
To:
CC:
Subj: My viewpoint

b6
b7C

First, a couple points related to your message. I really am not quite sure of who you are (all that matters is your experience - which is evident by your previous messages - not your name). I don't have your phone number, and would never call you (let alone harass you). I can assure you no one from Telenet would call you. As far as your allegations about the FBI, I personally have a good deal of respect for all law enforcement agencies; it is my opinion that they have a tough job in today's society, but I've never been on your current side of the fence. I am not with the FBI, I have worked for GTE for a number of years, and am very involved with the Telemail product - of which I am very proud and probably even a little protective or defensive.

I wanted to have a dialogue with you primarily for the benefit of Telemail and the industry in general. You have been involved with the current technologies and I am quite interested in your perspective. How vulnerable are today's systems (naturally I am not without an opinion), how would unauthorized access be best prevented, etc. I am not trying to play tricks with you - honest! Actually, I am very appreciative of your time and effort and feel you have a good deal of valuable input - if you are so motivated. The way I have approached our relationship is that if you are playing tricks on me, so be it, I tried. If you are helping me, I am only too happy to pass this along to the FBI, and maybe it might help me (naturally, I am not in a position to even suggest that it might help -- but I would like to think it does).

I am glad that you are not using an intermediary. That was your call, and I'm sorry you think it didn't work out for you. Also, I have not received a copy of "2600", but would really like to (of course you can't compare the mail to Telemail in terms of speed).

Thanks for your help. I hope we can really get into it.

[redacted]

b6
b7C

Posted: Fri Jan 13, 1984 2:31 PM EST Msg: LGIE-1597-4841
From: [redacted]/PH.PHRASES/ASSOCIATES
To:
Subj: RE: My viewpoint

I believe in your integrity and sincerity. I wasn't implying that I didn't trust you -- I was simply trying to point out how difficult it's become to trust ANYBODY. That's one thing I've learned from this whole thing. Any time you say or do something, it's always possible that there's somebody taking note of it. Until recently, I would have thought such a statement indicative of a paranoid, but now I'm not so sure.

I don't know if you realize or desire this -- but since my intermediary turned out to be an informant, that means every word that's passed between us has been looked at by many others. Now I don't have any problem with

this, but I thought you should know, in case you didn't already. Like I've said before, I'm very distressed by that revelation, most of all because that person was trying to get me to do all kinds of things on all kinds of systems. Fortunately, I didn't take him up on that offer.

Anyway, enough of this; I'll start working on the next real message now.

Manny

Posted: Sun Jan 15, 1984 4:59 PM EST Msg: AGIE-1597-5766
From: [redacted]PH.PHRASES/ASSOCIATES
To:
CC:
Subj: GETTING RID OF HACKERS

b6
b7C

What can be done to eliminate hackers on the Telemail system? Realistically, very little. Telemail is a huge system and not all of the certified users can be expected to follow the same strict guidelines for protection, or even to understand them. Hackers thrive on this sort of attitude, an attitude that won't change until the average user is injected with a little "hacker mentality" himself.. Once somebody sees what their weak points are and how these can be used against them, their protection will become more effective. [Example: penetrating a hacker's account would be much more difficult than penetrating an average account. Most hackers know how and where to protect themselves because they know how their own minds work. System operators are expected to possess this same foresight, and many times they obtain it through active experience.]

Since the vastness of Telemail will never totally disallow hackers, the primary interest should be to limit the damage they can do [accidentally or intentional] once they are inside. Right now, if I were to gain access to an account, I could not only see all of the names that I can send to, but thousands that I cannot send to. If I cannot send to these people, why should I even know they exist? With this kind of a system, I can get a hardcopy printout and spend days going down the list finding defaults (or, now, finding inactive accounts that never changed their defaults) or first-name or even user-name passwords. With each account penetrated, more names could be found. As I've mentioned in previous messages, there are other ways to get names using identity codes, a process that shouldn't be allowed.

Administrator accounts will be penetrated in the future. Not as often as in the past, perhaps, but it will happen. Major commands -- deleting or adding users -- should be subject to verification before they're acted upon, perhaps by generating a message to the administrator's real-name account, advising him/her of what is about to be done. (On this subject, I've heard reports concerning how all of those NASA users got deleted. Supposedly, a hacker was playing with one of the administrator commands and thought he would eliminate the termination dates. So, when he was asked for the termination date, he hit a return, thinking that that would leave it open. Instead, it made the termination date NOW and promptly eliminated all of the users in question. I can't confirm this -- administrator functions aren't my specialty -- but if it is true, it indicates a significant problem with this command, i.e. the same command can be made accidentally by a legitimate administrator.)

I'm not sure what the criteria is for allowing use of the SET command, but it can be used to cover up one of the best protective devices currently on Telemail, namely the last access date. This tells a person if someone else has been using his account. However, it can be suppressed using the SET command. A naive or inexperienced user might not notice or think that something is wrong with the system when he doesn't see the last access displayed. I don't see any positive application of this suppression; it's only one line in the first place.

Users should know if someone is trying to get into their account. If someone tries, say, nine times to enter a password for a particular user id, a message should be sent to the user, informing him of this, perhaps even letting him know what passwords were tried, in case the hacker is getting close. At the same time, the account should lock itself for a period of time, so that the hacker can't eventually guess right and it should re-lock itself if future attempts are made. But the hacker shouldn't be told that he's locked out, most importantly because such a message would confirm that he had a correct user id.

I'm sure there is more on this subject that I wanted to address, but I have to be somewhere else now. I'll devote some thought to anything else I want to add, and hopefully I'll get to that late tonight. Please let me know if you have any questions on the above or topics you'd like me to go over.

By the way, I'm now using my semi-local access number, as requested.

Manny

Posted: Mon Jan 16, 1984 3:17 AM EST Msg: EGIE-1597-5872
From: [redacted]/PH.PHRASES/ASSOCIATES
To:
CC:
Subj: SOMETHING ELSE

b6
b7C

Thanks for the compliment.

One additional item just came to mind... A function on the Telemail system that is nothing short of a hacker's dream is the Unread command. I had trouble believing that one when I first came across it. It was actually possible to read someone's mail and then reseal the envelope, without leaving ANY traces! I really have to think hard to find an over-the-counter use for that command. I'm sure there must be some purpose to it, but the misuse of the Unread function, in my opinion, negates that considerably.

I don't want you to get the wrong idea. Neither I nor the people I communicated with spent a great deal of time reading other people's mail. Yes, we did it a couple of times, when we suspected that it might have been really interesting (like with AT&T Long Lines (ATT.LL) and their clever password of BELL -- can you blame us?) but for the most part we stayed out of other people's affairs. More on that later.

What I'm trying to say is that if anyone really nasty and malicious got onto the system who KNEW what he was doing, the Unread command would be one of his closest friends. That, combined with the SET function I described earlier could very effectively cover his tracks.

One more thing: a notice of some sort when there is more than one user in an account should be seriously considered. There could be fifty people in my account right now and I'd never find out about them.

If I think of anything else, I'll pass it along.

Manny

Posted: Mon Jan 16, 1984 3:54 AM EST Msg: EGIE-1597-5874
From: [redacted]/PH.PHRASES/ASSOCIATES
To:
CC:

b6
b7C

On the lighter side, there are all kinds of interesting commands and features on this system. Some of which you may or may not be aware of. Odds ar most people don't know about this one.

*** Exception: This erro[redacted]hould not occur.

909 173 DISCONNECTED 00 20 00:00:20:18 43 96

@C 909173

909 173 CONNECTED

User name? [redacted] b6
Password? b7C

Welcome to TELEMAIL!
Your last access was Monday, Jan 16, 1984 9:34 AM

No new mail.

Command? RESUME

OK!!

It's a pretty interesting feature overall! I learned it from somebody on the system (a hacker, of course). I don't really see a purpose to it, except to create practical jokes and scare people to death. If I recall correctly, we did use it to successfully frighten away some rather inexperienced hackers. It was very effective, I believe.

ATTENTION HACKER. T
HIS
IS THE FBI AND WE HAV
E
TRACED YOUR CALL.

They haven't stepped on any sidewalk cracks since then, I hear.

I'll send some more serious stuff either late tonight or tomorrow.

[redacted]

Posted: Wed Jan 18, 1984 11:46 PM EST Msg: OGIE-1998-2476 b6
From: [redacted]PH.PHRASES/ASSOCIATES b7C
To: [redacted](RECEIPT)
CC: [redacted]
Subj: A PROBLEM WITH OUR COMMUNICATION

Hello,

As you know, I sent you a message a few days ago explaining why our communications had been temporarily cut off. In that message I told you that I was using a go-between who later turned out to be an FBI informant. I also made reference to the fact that I was being harassed and that I believed this informant was at least partly responsible.

Recently a message from this person was forwarded to me. In it, he vehemently denied those possibilities. Now then, since I have been careful not to talk with anyone else concerning this, I can only assume that he somehow read my message.

There are a few possibilities here. One is that the FBI is monitoring your system without your knowledge, in which case I feel an obligation to

tell you about it. Another possibility is that they're monitoring my which doesn't involve you at all. Or perhaps you're showing these communications to them yourself.

As I've said (or certainly implied) before, the latter possibility doesn't upset me at all. It's completely within your rights to share our conversations with anyone you desire; it's your system and it's your case. But think of this: somewhere along the line, no matter which of these three scenarios is true, the FBI is letting one of their informants read what's going between us!

Maybe I'm over-sensitive; I think, though, that you should be as indignant as I am concerning this. That person is not an FBI agent, and as far as I'm concerned has no business reading our mail - he is not the one conducting the investigation.

I'm really rather surprised at the FBI. I thought for sure they'd have policies against this kind of thing. By doing this, they're compromising their own security as well as ours - this person is not to be trusted with anyone! Having talked personally with him on a number of occasions, I've heard a few rather interesting remarks he's made which lead me to believe that he's no more on the side of the FBI than he is on mine. I think he's taking everybody for a drive. Of course, I could never prove this.

Please take whatever action you can to see that this unauthorized eavesdropping is stopped. I have nothing against authorized eavesdropping, but we should let it stop there. Please let me know your feelings on this.

Manny

P.S. Did you get my last message o.k.? I hope it didn't mess up your terminal or anything.

Posted: Thu Jan 19, 1984 8:04 AM EST Msg: FOIE-1598-2545
From: [redacted]/PH.PHRASES/ASSOCIATES
To: [redacted]
CC:
Subj: THE OTHER GUY

b6
b7C

I think the situation is less insidious than you might have assumed. The intermediary you used is also an experienced hacker (or so I believe). When he sent me a short message saying that he would not be an intermediary, I offered him a place out of the rain, so to speak, and gave him an account on Telemail. I need all the help I can get, and while I don't have the time or the inclination to play you two against each other, I can always use more information about my system and hackers. When you told me you thought he was an informant, I told him (electronically) that he was indeed viewed in this light, and he might want to clear the air if this was not based in truth. (I would think you would want this opportunity if you were in his shoes). Sorry, if this caused you undue concern, but I must admit all the possibilities you outlined could have been the case. As far as I know, the FBI is not monitoring my lines. It would be quite difficult technically for this to be the case.

I told you in a previous message that if the information you gave me was helpful, I would be happy to pass this along to the FBI (I think this cannot hurt you at all). Unless I hear differently, I will continue on this course.

Please discuss this further if you still have concerns about our communications.

b6
b7C

Command?

CAHN WISHOD & WISHOD
ATTORNEYS AT LAW
534 BROADHOLLOW ROAD - CB 179
MELVILLE, NEW YORK 11747
(516) 694-2300

RICHARD C. CAHN
EUGENE L. WISHOD
JOSEPH H. WISHOD

EUGENE R. BARNOSKY
DAVID R. JAMPOL

November 7, 1983

[redacted], Special Agent
Federal Bureau of Investigation
Hauppauge, New York 11788

Dear [redacted]: b6 b7C

Pursuant to our conversation of Friday, November 4th, I deliver to you on behalf of State University of New York at Stony Brook, various material relating to the computer investigation and [redacted] which I briefly outlined to you by telephone.

I would be obliged if, pursuant to our understanding, you would identify yourself to my secretary as Special Agent of the FBI and acknowledge receipt of these materials on the attached xeroxed copy of this letter.

Sincerely yours,

[redacted] b6 b7C

[redacted]

RCC:bp
Enc.
HAND DELIVERED

NW 65 Serial E-7

THE ABOVE MATERIAL WAS RECEIVED
THIS 7th DAY OF NOVEMBER, 1983

F-50

[redacted] b6 b7C

Office of Vice President for Administration
State University of New York at Stony Brook
Stony Brook, NY 11794
telephone: (516) 246-6000

Stony Brook

MEMORANDUM

To: [redacted]

From: [redacted] b6 b7C

Subject: FBI Search of WUSB Offices

Date: October 14, 1983

Pursuant to your request, I shall attempt to provide you with a summary of the events of October 13, 1983.

At approximately 1 P.M., I received a phone call from [redacted] informing me that there were several FBI agents on campus and presently were in the process of searching room 240 of the Student Union Building which was the studio of Station WUSB. He said they had arrived on the campus a couple of hours prior to this time armed with a Federal search warrant. He had assigned [redacted], a Public Safety officer, to accompany the agents. [redacted] advised me that he had called the President's Office as well as [redacted]. b6 b7C

I then met with [redacted] in his office and requested a copy of the search warrant. I noted that the search warrant limited the search to room 240 of the Student Union Building and asked [redacted] if that was in fact the room they were limiting their search to. He attempted to contact Stafford by radio while I was there to no avail. b6 b7C

Upon return to my office, I called WUSB with the intention of speaking with [redacted] who I was told was at a meeting. Instead, I spoke with [redacted], who advised me he was a former student and volunteer working with the station. [redacted] told me that he had a receipt for the items which the FBI took and brought it to my office accompanied by two other gentlemen who work at the station. b6 b7C

I am informed that there are only four members of the station's staff who use the computer, namely [redacted], and [redacted] of the station. [redacted] said that the room is always kept locked and that only the aforementioned people have access to it. b6 b7C

He told me they use a Heathkit H89 computer for the purpose of doing programming, listing of addresses, etc. I asked if they had done any programming on the computer or hooking into outside computers, since the warrant indicated that the evidence the FBI was seeking was with regard to wire fraud. [redacted] told me that at times they had made connections with "computer bulletin boards". I understand these bulletin boards are operated by computer hobbyists and are used for leaving messages for private people or retrieving technical information, etc. He said the bulletin board phone b6 b7C

b6
b7C

numbers are available in computer literature.

[redacted] told me that the agents advised him that the equipment was to be taken to New York City.

b6
b7C

Upon return to my office, I called University Counsel's Office immediately and advised them of the situation. I have forwarded to them a copy of the search warrants as well as the receipt for equipment.

On the morning of October 14th, I met with [redacted] and [redacted] described the incident as follows:

b6
b7C

At about 11:15 or 11:30, he was called by [redacted] and informed that the FBI was at the studio to search room 240. [redacted] asked to see identification since the agents did not offer credentials themselves.

b6
b7C

The agents then searched room 240, finding nothing that was computer related. [redacted] offered the information that we in fact did have computer equipment, but it was housed in room 227. The agents then made several phone calls and eventually requested permission to gain access to room 227 from [redacted]. He gave them the authority to enter and search that room. [redacted] accompanied the agents as did [redacted] of Public Safety. [redacted] then taught a class and had a meeting returning to the studio at about 3:30.

b6
b7C

[redacted] advised me that all of the computer hardware belongs to an individual named [redacted] and the software, discs, stationery, etc. are the property of Polity. Accordingly, it appears that nothing that was taken by the FBI is actually owned by the University.

b6
b7C

[redacted] spoke with the owner of the equipment, [redacted], and advised him that he would do well to seek legal advice. [redacted] was informed that at the same time this search was occurring on campus, there was also a search of [redacted] home in [redacted] was not there at the time but was advised by his roommate, [redacted], that all computer related equipment and software were removed from the premises at that time. [redacted] did not inquire of [redacted] of his involvement, but merely told him to seek legal advice. Subsequent to my meeting with [redacted] and [redacted], I spoke with [redacted] and [redacted]. I advised both of the new turn the situation had taken in that property was not that of the University. [redacted] felt that although that was the case, we were still peripherally involved since it was WUSB offices which they searched.

b6
b7C

b6
b7C

[redacted] had suggested, prior to learning that the equipment was privately owned, that [redacted] telephone the FBI and request that the equipment be returned to the campus and/or we get copies of everything they took. I forwarded this suggestion to [redacted] who said he would act on it.

b6
b7C

[redacted] expressed concern, as did [redacted], that neither my office nor University Counsel's Office was contacted by Public Safety when the agents first came on campus but only told several hours later.

b6
b7C

[redacted] also expressed the concern that he had no prior knowledge of the agents arrival. He felt that a phone call from Public Safety prior to the agents coming into the Student Union would have eased his situation greatly.

b6
b7C

[redacted] expressed some concern over the role of Public Safety in that he felt they should be more concerned with protecting the University rather than assisting the law enforcement giants of the FBI.

b6
b7C

RWN:jkw

att. (2)
1. Search warrant
2. Receipt of items taken

blcc: [redacted]

b6
b7C

nited States District Court

UNITED STATES OF AMERICA

v.

PREMISES KNOWN AS ROOM 240 OF THE STUDENT UNION BUILDING (BUILDING 37) LOCATED AT THE STATE UNIVERSITY OF NEW YORK, STONY BROOK, LONG ISLAND, NEW YORK

SEARCH WARRANT

CASE NO.

TO: ANY SPECIAL AGENT OF THE FEDERAL BUREAU OF INVESTIGATION AND ANY AUTHORIZED UNITED STATES OFFICER, OR ANY DEPUTY UNITED STATES MARSHAL

Affidavit(s) having been made before me by the below-named affiant that he has reason to believe that (on the person of, or on the premises known as) ROOM 240 OF THE STUDENT UNION BUILDING LOCATED AT THE STATE UNIVERSITY OF NEW YORK, STONY BROOK, LONG ISLAND, NEW YORK

in the [redacted] District of [redacted] there is now concealed certain property, namely computer and computer accessories, including but not limited to: CPU, terminals and keyboards, printers, disc drives, tape drives and other input/output peripheral equipment; including but not limited to magnetic tapes, discs (hard or floppy); all output products by or caused to be produced by a computer including printer output, teletype output or paper tape output; all notes, papers, notebooks, or any other type of information with or related to computer usage, including manuals, books, data sheets, diskettes, directories or any other device used to record information, addresses and listings of unauthorized usage or users of computer networks; and other drugs, papers, ledgers and monies which are the fruits, evidence and instrumentalities of crimes against the United States, that is, wire fraud, in violation of Title 18, United States Code, Section 1343;

and as I am satisfied that there is probable cause to believe that the property so described is being concealed on the premises above-described and the grounds for application for issuance of the search warrant exist as stated in the supporting affidavit(s).

YOU ARE HEREBY COMMANDED to search on or before [redacted]
(not to exceed 10 days) the person or place named above for the property specified, serving this warrant, and making the search (in the daytime — 6:00 A.M. to 10:00 P.M.) (at any time in the day or night as I find reasonable cause has been established) and if the property be found there to seize it, leaving a copy of this warrant and receipt for the property taken, and prepare a written inventory of the property seized and promptly return this warrant to [redacted]

[redacted]

Name of affiant

[redacted]

b6
b7C

* If a search is to be authorized at any time in the day or night pursuant to Federal Rules of Criminal Procedure, insert facts justifying such search in the affidavit.

** United States Judge or Judge of a State Court of Record.

RETURN

WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH
3-83	10-13-83 12:35PM	[redacted]

b6
b7C

INVENTORY MADE IN THE PRESENCE OF

[redacted]

INVENTORY OF PROPERTY TAKEN PURSUANT TO THE WARRANT

MAC
FLIP N FILE W/39 DISKETTES
ARC " " W/49 DISKETTES
ZENITH WINCHESTER DISK DRIVE (C:SY2)(Serial# 2-67 J237 M018 L07445.5)
HEATHKIT FLOPPY DISK SYSTEMS (SIDE, SY4: SY5) (MODEL H-77-2)
CHRONOGRAPH (#04110 4743)
SMARTMODEM (#0820 94002)

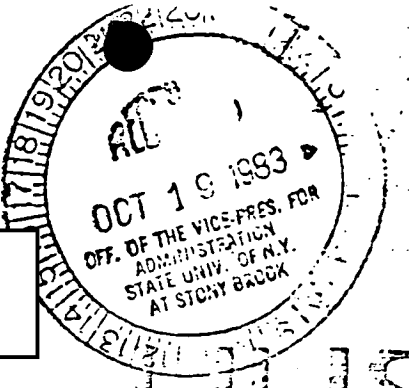
HEATHKIT COMPUTER (SY3/D)
MODEL H19-2, SERIES NO. 02-4399)
DIABLO 630 (SERIAL #(044) LARGE PRINTER
OKIDATA 92 & MICROLINE (Model 82A, Serial #215770) SMALL PRINTER
FILE JACKET CONTAINING MAILING LISTS
FILE JACKET CONTAINING COMPUTER NUMBERS
FILE JACKET CONTAINING DIGITAL RESEARCH
FILE JACKET CONTAINING BASIC LISTINGS
1 SHEETS CONTAINING NAMES + ADDRESSES
BOX OF MISC PAPERS + PRINTOUTS
ADDRESS WHEEL
ENVELOPE CONTAINING 3 5¼ DISKS

CERTIFICATION

I swear that this inventory is a true and detailed account of all the property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date

U.S. Judge or Magistrate



WUSB
99.1fm stereo

To: [redacted]

From: [redacted]

b6
b7C

Date: October 17, 1983

Re: Computer search by the F.B.I.

At approximately 11:30 a.m. on Thursday October 13, 1983, while in my office (Stony Brook Union 271), I received an intercom message from [redacted] b6 b7C that he was in the studio (Union 240) and there were agents from the FBI with him and I should come right down.

I walked into the studio and immediately identified myself to one of the agents (it wasn't until about 20 minutes later that I realized the agents had not identified themselves to me so I asked one to do which he did). They were accompanied by a member of the SUSB Office of Public Safety who you later identified to me as [redacted] (sp?). b6 b7C

Upon my arrival, they showed me a search warrant for computer related equipment and miscellaneous documents which they believed were located at the radio station (Union 240). I immediately became concerned over the fact tha I was certainly aware of computer equipment located on "radio station" premises but not in room 240. After a few minutes of the agents searching the first of several rooms in our studio complex, I decided that in order to prevent possible disruption, interference or tampering with present or future broadcast studio operations I would advise the chief agent, [redacted] that the station did have access to computer equipment which was located in another room of the Stony Brook Union. This equipment is personally owned by [redacted] at WUSB, and is used by the radio station to create and generate program logs, mailing lists and word processing documents. b6 b7C

At this time, [redacted] began placing a series of phone calls in order to get permission to search room 227. At the same time he asked me if I had authorization to enter room 227 and would I sign a statement stating such, which I did. At approximately 12:40p.m., the agents moved to room 227 (I

don't know if telephone authorization to do so had been reached). At this time, the agents entered room 227 which I had now opened for them and one of them immediately began photographing the contents of the room. Since I had to go teach my THR 270 class in the Fine Arts Building from 12:45-2p.m., I left the agents in the presence of [redacted], a station staff member and former [redacted] and now an alumnus of Stony Brook. Eric is authorized to have key access to room 227 as well as having knowledge of what computer equipment was in the room and could verify the "checklist" of equipment removed. b6 b7C

At the conclusion of my class, I went directly to the office of [redacted] and advised him briefly of the situation. b6 b7C

At our 9:30a.m. meeting on Monday October 17th, I advised you that [redacted] had come to me with information possibly pertinent to to the situation. In a later telephone conversation you suggested that you would schedule a meeting with him and other campus officials. b6 b7C

xxx 8242

October 19, 1983

[redacted]
Office of University Counsel
State University of New York
State University Plaza
Albany, NY 12246

b6
b7C

Re: FBI Computer Search

Dear [redacted]:

Enclosed please find a copy of [redacted] account of the events of October 13, 1983, as well as a mention of his conversation with [redacted], which occurred in Port Jefferson on October 15, 1983.

b6
b7C

On October 18, 1983, at approximately 2 P.M., [redacted] Officer, and I met with [redacted] concerning additional information, which he had conveyed to [redacted].

b6
b7C

[redacted] is a full-time student at Empire State College and is taking one course on our campus. He is [redacted] at WUSB. [redacted] stated to us that when the FBI agents arrived, he thought it necessary to advise [redacted] of their presence, in that he knew they were interested in the computer equipment and thought [redacted] was the owner. He said he telephoned [redacted] at home shortly after the agents arrived on the scene, and [redacted] responded, "Thanks a lot for letting me know, there are things we have to get rid of." (Or words to that effect.) In addition, [redacted] told us that [redacted] is a telephone buff, as it were, and is very knowledgeable about technical aspects of the telephone and all of its various ramifications. He also stated that at one time, he, [redacted], was present when [redacted] and a couple of other young men were apparently making a telephone call to the Defense Department in Washington. He stated that although he has no technical knowledge of the computer, he was present when he thought that [redacted] and [redacted] were apparently gaining access to some computer outside the University, though he did not know what or where at the time.

b6
b7C

[redacted] also noted that several times during the summer, he heard [redacted] and [redacted] comment about fear of the "phone police" arriving, and that he inferred from these comments that they were doing something illegal with the telephones.

b6
b7C

[redacted] is an alumnus of Stony Brook and was involved in a similar incident concerning the computer at Catholic University of America in Washington. I am enclosing the records, which we have on that case for your information and files.

b6
b7C

[redacted]

b6
b7C

At the present time, we are attempting to find out if the telephone lines on campus were used illegally or for the purpose of accessing our own Univac. If that investigation yields any fruit, I will keep you advised.

Very truly yours,

[redacted]

b6
b7C

RWN:lm

Enclosure

cc: [redacted]

b6
b7C

STATE UNIVERSITY OF NEW YORK
AT STONY BROOK, NEW YORK

Memorandum

To: [redacted]

From: [redacted]

Date: 7/29/81

b6
b7C

.....Appropriate action

...../.Comment and criticism

.....Your information and files

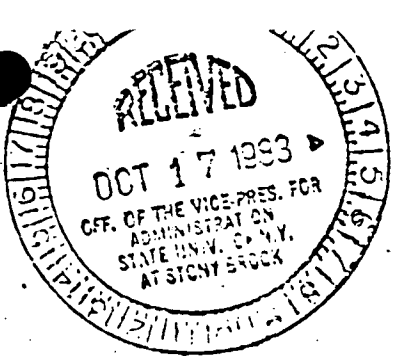
.....Please note and return

.....At your request

[redacted]

[redacted]

b6
b7C



STATE UNIVERSITY OF NEW YORK
AT STONY BROOK, NEW YORK

Memorandum

To: [redacted]

From: [redacted]

Date: 7/29/81

b6
b7C

.....Appropriate action

.....Comment and criticism

.....Your information and files

.....Please note and return

.....At your request

[redacted]

Re. [redacted]

You can file this. I think the case is closed.

b6
b7C

July 21, 1981

TO WHOM IT MAY CONCERN:

The following is a concise account of my dealings with the computer at the Catholic University of America and the events which led up to it.

In early March of this year, a video computer terminal was obtained by a friend of mine. It was purchased with the original intention of helping him with homework in a course he was taking. However, we both anticipated eventually using it for record catalogues on WUSB-FM, the campus radio station which we both work on. For this reason the terminal was kept for a time in our technical office.

We wanted to find out as much as we could about the different types of systems available so that when the time finally came to start entering our data (which would be record titles and companies), we wouldn't, in effect, be stumbling in the dark. We found out about a local computer bulletin board, located in Centereach, called Connection-80. What a computer bulletin board does is list the access numbers of computers all around the country where one can either leave messages for other callers or obtain information about various computers.

The access number for the computer at Catholic University was listed on this bulletin board and probably on many others. I must stress that there is nothing underhanded about this particular point, since the number was given to this bulletin board by the computer club at Catholic University. It was meant to be called. This is what we did, with absolutely no evil intentions whatsoever. We dialed into their system to obtain information, which we were invited to obtain by their having the number available.

When we made the initial connection to this computer, I recognized it as the same type of computer which was used in my high school. I remembered a few commands and one of them was the SEND command, which would allow the user to instantly send messages to other users. However, I soon realized that there was a major difference between the two systems. The one which I had used in the past was unable to send messages unless the user was logged on. What this means is that the user had to enter his account number and password before he was able to do any sort of work, which included sending messages. Even then, he was only able to send messages to those who wanted messages sent to them. Catholic University proved to be quite different. Anyone who dialed into the system could send messages to anyone else without being logged on at all.

Out of curiousity, we tried to make contact with other users, to see if this really worked. Several responded, saying that they didn't want to be bothered. We complied with their requests. A couple of others wanted to talk us, including one person whose first name was [redacted] (or so he claimed). His last I couldn't remember except that it had one syllable. The reason why he stands out in my mind is because he asked so many questions. I gave him my name, my major, the school I went to, the telephone number for the radio station, and all sorts of other information which I didn't see any harm in giving him. At one point he asked for my home phone number and address, which is where I drew the line. I did, however, give him the access number for the computer at Stony Brook, perhaps foolishly, although I honestly didn't see what harm he could do with out a password or account number. At another point, he suggested (since he knew that I was [redacted] of a radio station) that I trade him records for account numbers and passwords into his system. At the time I took this as a joke and I don't believe I

b6
b7C

.en responded.

I talked to this same person the next evening (I don't remember the exact date except that it was sometime in March) and possiblt the evening after that as well, which would have been the last time I called up their system. On each occasion he asked me questions about myself and what I did. I asked him a few questions as well, however, in all honesty I forgot his answers in a matter of hours, since I had slightly more important things on my mind. Unfortunately, we don't have a printer, so the communications I had with this individual were lost as soon as they left the screen on the terminal.

That is the extent of my dealings with the Catholic University computer. At no time did I log on to their system and I certainly never offered to make any deals with anyone for such an opportunity. Frankly, I wouldn't know what to do even if I was able to log on. I know very little about computers and I don't have a great desire to expand that knowledge, except to know what kind of a system would be good for our record catalogues. My experience in high school was minimal, to say the ~~xxxx~~ most.

I really don't understand what has been going on since I communicated with this individual. In early May I heard from the office of our Vice-President for Student Affairs. They told me that they had a complaint from Catholic University ~~xxxxx~~ which concerned me. When I first heard this, I was extremely annoyed. I felt that anyone who saw harm in my few communication with random users was extremely paranoid.

Since then, though, I have become more aware of the facts involved. I have spoken with both the afore mentioned vice president as well as the campus judicial officer and, from what they have told me, Catholic University has a very legitimate gripe. Someone has been communicating with users attempting to obtain passwords and other secret information. Perhaps this is not so unusual; I'm not familiar with the espionage dramas that I've been told exist behind the doors of the computer room. What is unusual (at least, in this particular case) is that my name has surfaced as the one trying to obtain all of this valuable information. As I mentioned before, I have no interest in these things, and even if I did, I don't have ~~xxxx~~ the time to devote to it.

What appears to me to be happening is that some inconsiderate person is attempting to rob the Catholic University of its computer services and is using my name in the process. (It's obvious he/she wouldn't use their own name!) In this case the person had previously found out all sorts of things about me so that they could be more convincing. Well, they were. I haven't seen the copies of the conversations that occurred, but I'm sure I would be shocked to see someone use my name and personal information while attempting to rip someone else off. Shocked and a little scared. Not to mention angry.

I want to see this stopped and if we can prosecute the person responsible, great, but I really doubt we can do this unless we start tapping phone lines or something. In any event, what I would suggest to the Catholic University is to tighten up their security a little, so that it's not so easy for non-users to communicate with users. And if anyone in the future is found to be using my name, in any form, I want to be notified directly. Thank you.

Sincerely,

[redacted]

b6
b7C

StonyBrook

State University of New York at Stony Broo
ng Island, NY 11794
telephone: (516) 246-7000

June 24, 1981

[redacted]
Computer Center
The Catholic University of America
Washington, D. C. 20064

b6
b7C

Dear [redacted]:

Following receipt of your May 1st letter and the attached records on [redacted] interaction with Catholic University's computer, we have consulted with legal counsel and with our campus Computer Center. We have concluded that [redacted] actions at this end do deserve limited action under our campus judiciary code, but do not deserve criminal proceedings instituted by Stony Brook.

b6
b7C

The University's legal counsel suggests that there may indeed have been a criminal offense directed toward Catholic University through theft of time on your computer. However, our counsel further states that Catholic University should be the party making a determination on whether criminal proceedings should be instituted in this case.

[redacted], reviewed the material you forwarded with members of his staff. He noted that there was interaction initiated by [redacted], but he also noted that that interaction was available through straight telephone access and that none of the reported conversations included any requests to [redacted] to get off the line; none of the reported conversations indicated that [redacted] was bothering the users with whom he was conversing or was hampering their operations.

b6
b7C

We will be charging [redacted] with unauthorized use of University services. We will certainly make it clear that from our standpoint his behavior was inappropriate and violated our Student Conduct Code in more than one way.

b6
b7C

You may also wish to know that the terminal from which [redacted] was operating has been removed from the radio station. It was a personal machine belonging to another student. It was to have been used for developing record files. Any such development in future will be strictly monitored by the general manager of the radio station.

I appreciate very much your willingness to share with us the full report of information that you had about [redacted] inappropriate interaction with your computer. Please let me know if we can help you in any other way.

b6
b7C

Very truly yours,

[redacted]

ELW:ajt
x.c.: [redacted]

Office of the Vice President for Student Affairs
State University of New York at Stony Brook
Stony Brook, NY 11794
telephone: (516) 246-7000

StonyBrook

MEMORANDUM

To [redacted]

From [redacted]

Subject Investigation of [redacted] case

b6
b7C

Date June 18, 1981

At your request I have pursued the matter of [redacted] use of a computer terminal in WU[redacted] to access the computer at Catholic University in Washington, D. C. I have consulted with [redacted], University Computing Center, and [redacted] has graciously reviewed the case and consulted with several members of his staff. [redacted] has reported to me that the log of the transactions sent to us by Catholic University does not show that [redacted] used criminal means to gain access to their computer. In fact, the way in which their system is set up, they permit access without a password. [redacted] also added that there is no evidence that anyone at Catholic University ordered [redacted] to get off the computer or in any way indicated he was bothering them or hampering their operations. From [redacted] perspective, we should focus on [redacted] unauthorized use of University telephone lines; his questionable offer to trade property, which perhaps did not belong to him, to gain access to another system; and his foolish interference with computer operations at another university.

b6
b7C

Based upon this review, I feel that [redacted] should be charged under the University Student Conduct Code and receive a letter of warning and disciplinary probation from the University Hearing Officer. I believe that this matter does not warrant further action.

b6
b7C

If you require additional information, please see me.

SRT/lp

x.c.: [redacted]

b6
b7C

Office of the Vice President for Student Affairs
State University of New York at Stony Brook
Stony Brook, NY 11794
telephone: (516) 246-7000

StonyBrook

MEMORANDUM

To [redacted] Computing Center

From [redacted] b6 b7C

Subject [redacted] Case

Date June 18, 1981

I wish to thank you very much for your help in the investigation related to the [redacted] case. Your review of [redacted] b6 b7C transactions has been very helpful and has enabled the University to determine how to proceed in this matter.

Thank you again for your cooperation.

SRT/lp

x.c.: [redacted] b6 b7C

State University of New York
State University Plaza
Albany, New York 12246

Office of the University Counsel
and Vice Chancellor for Legal Affairs
(518) 473-7591

JUN 10 1981

June 3, 1981

[redacted]
Administration 355
State University of New York
Stony Brook, New York 11794

b6
b7C

Re: [redacted]

Dear [redacted]:

I have reviewed the materials which you submitted in relation to Catholic University of America's complaints about attempts at unauthorized computer access made by an individual identifying himself as [redacted] at WUSB.

b6
b7C

Although the facts present a rather unique case, I concur with [redacted] analysis that the Rules of Student Conduct may be implemented in student disciplinary proceedings on campus. Since there is no specific category in the prohibited conduct section of the Code covering misuse of University telephone lines for the purpose of securing illegal computer access, I suggest that the alleged misconduct falls within the general sections relating to "Respect and Protection for Persons and Property" (Section A-1) and the "Integrity of Transactions and Records" (Section A-3).

More specifically, these sections provide that:

> "A(1)(b) No student shall take, possess or damage any property not his/her own on the University campus or on any University property."
>
> and
>
> "A(3)(d) No student shall knowingly take or use any services without authorization."

There may be other sections which you feel are more appropriately utilized than these cited. In any event, I see no jurisdictional difficulty.

June 3, 1981 b6 b7C

If I can be of further assistance, please feel free to contact me.

Very truly yours,

[redacted] b6 b7C

GJD:set
cc: [redacted] b6 b7C

CAHN WISHOD & WISHOD
ATTORNEYS AT LAW
534 BROADHOLLOW ROAD
MELVILLE, NEW YORK 11747
(516) 694-2300

RICHARD C. CAHN
EUGENE L. WISHOD
JOSEPH M. WISHOD

DOUGLAS A. McNALLY

RECEIVED
JUN 1 1981

II A 1b
3d

May 29, 1981

[redacted]

b6
b7C

Administration 355 - SUNY
SUNY at Stony Brook
Stony Brook, NY 11794

~~CONFIDENTIAL~~

Re: [redacted]

Dear [redacted]:

b6
b7C

I have reviewed the file on [redacted] and I believe that there was a criminal offense which probably in the last analysis will be determined to have occurred in both the State of New York and the District of Columbia. However, the victim of the theft, Catholic University of America, should really be the party making a determination where criminal proceedings should be instituted, if at all.

With respect to any student disciplinary proceedings on campus, I would assume something in the Rules of Student Conduct would cover a Stony Brook student utilizing the University telephone lines for the purpose of making long distance calls and securing illegal access to another university's computer. You should, therefore, consider whether as a matter of policy you desire to institute such Student Conduct Code proceedings against the student.

b6
b7C

[redacted] at Counsel's office has expressed a strong interest in this matter and I am, therefore, this date forwarding to her all of the materials which were just received from you together with the copy of this letter.

Sincerely yours,

[redacted]

b6
b7C

RCC:bp
cc: [redacted]

THE
CATHOLIC UNIVERSITY
OF AMERICA
WASHINGTON D.C. 20064

COMPUTER CENTER
202 635-5373

MAY 5 1981

May 1, 1981

[redacted]
Administration 355 - SUNY
State University of New York at Stony Brook
Stony Brook, NY 11794

b6
b7C

Dear [redacted]:

As I promised in our phone conversation Thursday, April 30, 1981, enclosed are copies of the pertinent dialog between three different CUA computer users and someone who has been accessing our DECsystem-10 claiming to be [redacted], an [redacted] at SUNY/Stony Brook and an employee of Radio Station WUSB. In the printouts, dialog beginning with ";;TTY56" is from the "phantom" caller, and dialog beginning with "SEND TTY56 ..." is from our user. (The number of the terminal, TTY56 above, may vary--this is because he was dialing into the system and getting a different line each time.) In most cases, his messages appear in lower case characters and our user's appear in upper case only.

b6
b7C

The problem was first brought to my attention Thursday, April 23, 1981, when one of our part-time programmers gave me a printout (see Item 1) of a dialog between himself and someone who claimed to be named Eric who was offering to trade record albums for an access code to our system. The caller claimed to be working for WUSB and using a terminal located in the station. He told of exchanging five record albums with one of our students named [redacted] in exchange for [redacted] access code to our system. When we checked the code he had been using, we found that it had not been issued to anyone named [redacted]. We did talk to the person to whom the account was issued and are fairly certain that he was a victim of someone on our campus using his access code.

b6
b7C

Friday, April 24, 1981, a graduate student brought me a printout (see Item 2), again of a dialog with [redacted], this time offering to trade access to long-distance telephone lines in exchange for a system access code. The caller gave our user a local phone number to call, two access codes for the communications system and instructions on how to use them.

b6
b7C

5.06.81
[redacted] called [redacted] - she will get back to him after consulting boss
" " [redacted] - boss returns call

 b6 b7C

At this time, I talked with a representative of C & P Telephone Company. After a check, he told me that the lines being used were not Bell Telephone lines, and therefore, they were not interested in the problem. I next talked to a [redacted], an investigator for MCI Communications. He was most interested and most concerned about this activity. He subsequently checked, however, and found out that the access scheme was not MCI, but was one belonging to Southern Pacific Communications. I talked with [redacted] of SPC. He told me that the long-distance access codes belonged to two California firms, and that they would begin to monitor the usage of the two codes. I sent him copies of some of the pertinent printouts. b6 b7C

[redacted] called me Thursday, after I spoke with you, to tell me that he had somehow examined the account activity for March for the two access codes and learned that [redacted] had made several calls using these codes. He also told me that he had talked with [redacted] of SUNY/Stony Brook and had confirmed that [redacted] was a student there. He indicated that no action had been taken. I gave him your name and phone number. I assume he has since contacted you. b6 b7C

Both firms expressed that while they are concerned about illicit usage of their phone lines by a person claiming to be a student, they are most concerned about the damage that could be done if the numbers were given to a "professional" who fully understood their usefulness.

Meanwhile, our Systems Programmer began taking steps to temporarily limit what a user could do on our system without having an access code. This patch was in use over the weekend, so we do not know what, if any, access this person tried to obtain. However, the patch had to be removed Monday morning and a more permanent fix applied. This was not accomplished until Thursday morning.

This person was again on the system Tuesday night. Both the user who "talked" to him last Thursday and our Night Operations Shift Supervisor engaged him in dialog over the system. Printouts from both dialogs are included. Our user this time managed to extract the last name of [redacted] (see Item 3) and also that he had used a DECsystem-10 while he was a student at [redacted]. Our Operator did not learn anything which we did not already know. b6 b7C

In addition to the events we can document with printouts, I have had numerous students, faculty and even staff members of the Computer Center tell me that they had at one point received unsolicited messages from this person. Unsolicited messages serve only to interrupt someones work and to distract them from what they are doing. In the case of one user, he had to reprint several pages of a document because a "garbage" message was in the middle of it.

 b6 b7C

The person calling himself [redacted] has twice given our people the phone number of WUSB. I know of one occasion when our user actually called the number, asked for and actually spoke with someone claiming to be [redacted]. b6 b7C

Of more serious import, Tuesday night during the dialog with our Operator, the caller gave him the phone number (see Item 4) to access your Univac computer system. I am sure that my counterparts in your Computer Center would be most interested in this.

We would like to see this activity stopped. As I have indicated, we have taken steps to tighten our own system security.

Clearly, this may be a situation in which the caller does not realize the seriousness of his actions. However, we estimate that we have spent over $1,000 in staff time alone dealing with this problem. We view this as harassment of our employees and our users. This activity, from our understanding, is a Federal offense if the calls are coming across state lines from New York to Washington, D. C. In addition, this person has admitted using SPC lines without authorization which is probably also a violation of statutes.

We appreciate your taking action on this problem. Please feel free to contact me if I may be of further assistance. I would appreciate your letting me know the outcome of this situation.

Sincerely,

[redacted] b6 b7C

[redacted]

AAH:mct

Enclosures

Communications Management Engineering
Office of the Vice President for Administration
South Campus Building A, Room 142
State University of New York at Stony Brook
Stony Brook, New York 11794
telephone: (516) 246-3500

StonyBrook

MEMORANDUM

To [redacted]

From [redacted]

b6
b7C

Subject WUSB Telephone Inventory

Date October 26, 1983

Attached is a listing of all telephone lines leased to WUSB Radio Station. The list is broken down into two categories, the first part consists of 6 telephone lines, only one of which is capable of reaching long distance (7122). Also attached is the billing for this phone from May, 1983 through September, 1983. The remainder of the phones cannot reach long distance, however, the two phones with A2N service can reach all of New York State and Washington, D. C. and vicinity. Unfortunately, our antiquated Centrex phone system is not able to identify calls made on these tie lines.

The second part of the list labelled radio circuits are used throughout the campus to interconnect various locations such as the Gym back to the studios to broadcast sporting events.

The potential for a bright technical oriented person such as the involved parties is to connect anyone of these radio circuits to any phone circuit on campus in the many Telco closets scattered throughout the campus. In effect this would mean they would be able to make calls from the studio via these circuits on anyone's phone line which in most cases goes undetected because very few department heads question their telephone bills on a thorough basis.

The Message Unit Detail (MUD) reports which I promised are still being processed by the phone company and should be available in about 1 week. This will give you all local calls made on these phones in the 516 calling area for approximately 6 months.

If there are any questions that may surface regarding the attached, please call me.

Attachments
DM:pvo
cc: [redacted]

b6
b7C

[redacted]

-PM
16 JAN

Robert Millikan
37c
USA

Federal Bureau of Investigation
ATTN: [redacted]
300 Lee Street Room 500
Alexandria, VA 22314

b6
b7C

F-74

HICKSVILLE, NY
PM
12 JAN
1984

SM

USA
20c

Roger Olson
[redacted]

NOT
7
CHICAGO, IL

January 14, 1985

[redacted]

Federal Bureau of Investigation
300 North Lee Street #500
Alexandria, VA 22314

b6
b7C

You called the other day to ask about a person named [redacted] As I told you then, I have received phone calls over and over and over again asking for this person.

Now today, the enclosed arrived in the office mail because the mailman couldn't find a box for it otherwise. I have to say of all the phone calls looking for him, its the first time a letter was addressed to him here. The address is not even correct, we don't have a number such as B-16.

If its of any help you are welcome to it. There is no return address shown to send it back to and I refuse to get involved any further by reading it or learning more about Roger. The less I know the better I feel. If anything further comes to my attention I will advise you.

[redacted]

b6
b7C

2600 • January, 1984!

Published monthly by 2600 ENTERPRISES, an eleemosynary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953

*0#D

VOLUME ONE, NUMBER ONE

AHOY!

(That's how Alexander Graham Bell used to answer his phone. For some reason, it never caught on...)

This is the very first issue of *2600*. We will, on this page, explain our motives and what the goals are which we hope to achieve with this publication.

The idea for *2600* was born early in 1983. We saw a tremendous need for some form of communication between those who truly appreciate the concept of communication: technological enthusiasts. Of course, others have different ways of describing such people—these range from words like hacker or phreaker to stronger terms such as criminal or anarchist. Our purpose is not to pass judgement. *2600* exists to provide information and ideas to individuals who live for both. **All of the items contained on these pages are provided for informational purposes only. *2600* assumes no responsibility for any uses which this information may be put to.**

Of course, a lot has changed since our first days. *War Games* came out. And then the 414 gang got caught. Suddenly everyone was talking about phreakers and hackers. And while there were some that sort of jumped into the limelight, others were a bit more cautious, in fact, some were quite upset. Sure, the publicity was fun. But what would be the cost?

Well, time has passed and the cost has been high. Phreakers and hackers have been forced into virtual isolation. Raids by the FBI have become almost commonplace. The one magazine that was geared towards phone phreaks (*TAP*) mysteriously disappeared at the height of the crisis, sparking rumours that they, too, had been raided. However, in November, the magazine resurfaced, with an explanation that a fire had destroyed part of their mailing list. (Incidentally, if your name was one of the ones that was lost, you can claim the issues you are entitled to by sending *TAP* a copy of their mailing label or a cancelled check.)

And then there was the legendary computer bulletin board known as *OSUNY*. Enthusiasts from all across the country called up this board and left messages ranging from the latest in Sprint codes to how to crash an RSTS system to what to do once you've finally gained access to Autovon. Within a week after being mentioned in *Newsweek*, *OSUNY* was disconnected. Word has it that they are still in existence somewhere, but by invitation only. A truly smart move, if that is the case.

Many hackers were keeping a low profile even before the October raids. When the FBI confiscated equipment from 15 sites across the country on the twelfth and thirteenth of the month (sponsored by a grant from the folks at GTE), many of our contacts were lost because they feared the consequences of continuing. Two organizations, the Inner Circle and PHALSE, were deeply affected by the raids. The latter group (whose initials signify Phreakers, Hackers, and Laundromat Service Employees) is still in contact with us on occasion and has promised to contribute many articles devoted to just what was really going on.

So it seems that the events of 1983 have conspired to actually *strengthen* the resolve of hackers and phreakers across the country to put out this monthly newsletter. We hope you will help us continue by subscribing, spreading the word among your friends, and of course contributing articles and information. Since we are non-profit, it really doesn't matter to us if you xerox your copy and send it to someone else—all we ask is that you let us know so that we can have a rough idea of how many people we're reaching.

2600 has several sections, some of which will appear every month, others on an irregular basis. On this, the front page, and on page two, you will always find informative full-length features on relevant subjects. Future topics include: "A Guide to Long Distance Telephone Services and Their Vulnerabilities", "DEC and Their Many Mistakes", "Phreaking in the Sixties", and "Tracing Methods Used by the Law", as well as any late-breaking items. "FLASH" appears on page 3 and provides a roundup of timely news items written from a technological enthusiast's perspective. Page 4 is used for a variety of things—interesting stories from the past, schemes and plots that just might work, and feedback from subscribers. The last two pages of *2600* are comprised of data. Just what sort of data, we cannot say. However, if it is something that you are looking for, then you will probably recognize it.

The three holes on each page serve a purpose. We suggest that you obtain a loose-leaf book so that you can neatly file every issue of *2600* you receive.

Many thanks to those of you who subscribed without even seeing an issue. A word of advice, though: don't do it again or you'll probably get ripped off! We'd also like to thank those who took advantage of our free issue offer. If interested in subscribing, the rates and address can be found at the top of this page.

Welcome to *2600*. Turn the page and become a part of our unique world.

FBI GOES AFTER ADS HACKERS

IBM must press charges before action can be taken — Feds reveal their tactics, blow source

On this page we had originally planned to run an article entitled: ESS — Orwell's Prophecy. *At the last minute, however, we received this bombshell from an anonymous contributor. It seems that a group of hackers was making use of one of IBM's ADS systems. (Audio Distribution Systems enable users with touch-tone phones to send voice messages back and forth to each other. Look for an in-depth article on them in a future issue.) Unfortunately, as is all too often the case, one of these hackers was really an FBI informant who was taking note of all of the illegitimate users (around 40 or so). Luckily for this particular group, the informant was sloppy and left many telltale clues which gave them literally months of warning. So, when the informant decided to send a message to the system operator, advising IBM to take action against the hackers and to call the FBI for more information, the hackers were ready. The system operator's account had also been penetrated by them and hence, the message was received by the hackers first! One of them actually followed the instructions in the message and called the FBI! And for some reason, the investigator there thought he was talking to an IBM executive. This is some of what he said.*

One of the individuals that supplies me with information from time to time has uncovered a lot of abuse within the ADS systems, not only here in the United States, but in England and Italy. I talk to this individual on a private bulletin board. . .

We have no ability to come in as an outside investigative or law enforcement agency and do anything about it because, first off, we don't have a complainant. We don't want to step on anybody's toes, but it's been our policy to monitor bulletin boards and the phone phreaking activity across the country and advise commercial computer systems and corporations if we do discover certain computers along with the passwords and account numbers being published on the board. We do this on a one on one basis.

The GTE Telemail Connection

That was my baby, too! As a matter of fact, that's how we came across the ADS system — through the GTE investigation. [These] people are not just interested in data communications through terminals — they will leave voice messages on an ADS. We have been slowly uncovering more and more on the ADS in the last two months.

The major phase of [the Telemail investigation] was about 20 individuals that we had located and identified and we're looking for indictments on most of them coming down in the next month or two. We're talking about a group of highly organized people that do communicate on a daily basis all the way across the country — from San Francisco and L.A. to Denver to upstate New York. So we have a core of individuals that we are still looking at that are using your system and then we have this peripheral that we are not as concerned about because they are not part of an out & out conspiracy or an organized network, per se. I know of at least 8 or 10 that are the central figures in this, the carryover from Telemail. And we keep hearing information of other people who are calling in with junk messages — there's no real substance to their messages. Now the reason I know that is that they have included one of my sources of information onto their system and so he gets messages from the other parties.

The Communist Connection

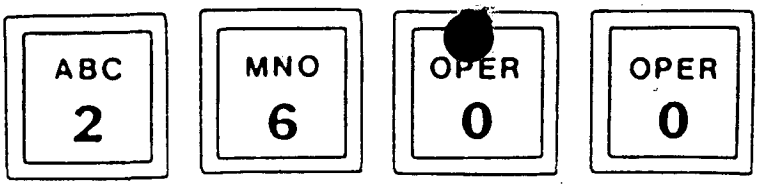
In a way we're somewhat fortunate that it's 16-year-olds or 26-year-olds as opposed to people from behind the Iron Curtain. It gives us the opportunity to see how these systems work and see if we can plug any loopholes before somebody from a not-friendly nation would try the same thing. I personally fully expect it — I'm surprised it hasn't happened in the past. It may have. We just haven't caught it. But the kids are a little bit sloppier and they're getting caught. . . I hate to sound paranoid, but we're supposed to be considering the big picture as far as is there anything sensitive in nature. For us within the bureau, sensitive in nature first off means national security and you've got corporate trade secrets and the like that you don't need being distributed.

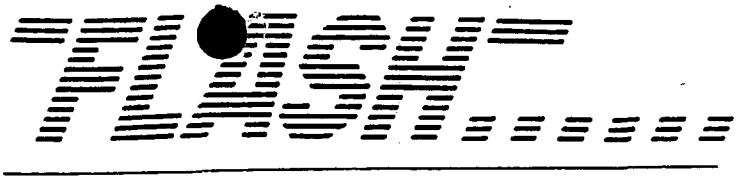
How the FBI Wins Trust and Gets Info

The subjects have an ego problem and they love to talk to other individuals about what they are capable of doing and bragging about it. They have a tendency to trade information. Everything is negotiable with them. We have never had to barter away access to systems — we do it more on the technical information of phone networks, computer systems, and the like to where it's more of a technical information tradeoff as opposed to an access tradeoff. [An example would be the] login procedure for a PDP-11. You integrate yourself within their confidence and their circle of friends. You feed them a little bit of bait and a lot of times they'll go for it. You enter into a dialogue with them and they end up taking you for a ride.

These people are very hungry for technical avenues through which they can communicate. It used to be the personal computer bulletin boards — public messages that anybody can read. You start finding out that they leave a phone number or an address — and you start finding out who the parties are. There's thousands of these bulletin boards across the country and you narrow in on maybe twenty or so that are the more hardcore bulletin boards that are being used for exchange of illicit information. Then they move from there to an electronic mail service, namely GTE

(Continued on back page)





GTE raids still have many unanswered questions—computer owners concerned

Combined News Sources

On Wednesday, October 12, at 6:00 AM, the FBI started to raid the homes of over fifteen individuals for allegedly breaking into Telemail, GTE Telenet's massive electronic mail service. While much of the publicity has now died down, questions remain concerning the legality and the overall implications of such computer seizures.

At a December 16 meeting of the Long Island Computer Association, this topic was addressed. Some members could not understand the rationale for taking away the computers in the first place. "It sounds like scare tactics to me. . . to keep these kids off of computers," one commented. "To hold the equipment seems like something that should be unlawful and it's something that the public should look at. If it's not justified, we should say that we won't put up with it anymore and to return the equipment." He did not elaborate on precisely what kind of action a computer group such as LICA could take.

Legally, the computers can be kept for as long as they are needed in the investigation. Ultimately, a judge will decide how long that can be.

"The allegation," said an attorney familiar with the case, "is that the services of the Telemail bulletin boards were used and the theory that the government is proceeding under is that it was a violation of Section 1343, wire fraud (a scheme with intention to defraud someone else using either television, telephone, or some other communications means). They're saying that if there was use of the bulletin board service, then that was a 'theft of service' and there was intention to defraud GTE."

One member took GTE's side. "These are all nice games these people are playing, but they are a theft of service. Somebody is in the business of providing that service and they're deliberately interfering with their providing that service. They're trying to get something for nothing."

Another disagreed. "You may be on their computer, but it's not costing them anything, if you're not taking up time. Unless the whole system is fully used and you were the last user on, are you really using any of their time? Really and truly?"

Many hackers felt they were unjustly accused. One even said he'd never used the Telemail system. Others said they had looked around once or twice but had never hurt anything. Others, though, admitted to deleting mail and playing tricks, like sending obscene messages back and forth between two innocent executives.

Whether or not the Telemail system was used fraudulently did not seem to be the overriding issue at the LICA meeting. What had members there worried was the way in which the investigation was being carried out. When dealing with computers as evidence, different rules apply, rules that for the most part have not been written yet. "Data can be manufactured just as easily as it can be erased from a personal computer," one member commented. "And the longer that they have the computer in their custody, the less likely that the information that they claim is on it was actually there. Because, as we know, you could enter any date, any time into the computer and have it date- and time-stamp the files."

Meanwhile, a GTE Telenet spokesperson said that the corporation still intends to prosecute and denied that the whole thing was being put on for the deterrent effect that it might have on other people. The spokesperson also said that abuse on the system was discovered in the past, but they didn't prosecute at that time. This time, though, they're serious.

AT&T Credit Cards Make Debut

2600 News Service

There's now another way to place telephone calls without dimes. This month, the "true" AT&T credit card phones are making their debut in various airports around the country. This new phone actually takes an AT&T credit card (not those wimpy "calling cards" or "PIN cards." We're talking about a *real* hunk of plastic, with a magnetic strip and everything.) — and there's even a little video screen that gives you directions.

Unless some sort of a bug can be found within the system itself, phone phreaks won't accomplish very much here, unless they can actually get their hands on other people's cards. This, in itself, wouldn't be too difficult, since large numbers of the cards would be sent out on the same day in a particular area. Stealing out of personal mailboxes, though, is an act most phone phreaks would never stoop to. And the folks at AT&T are well aware of this.

Wireless phones spell trouble

2600 News Service

With cordless phones popping up all over the place, problems were bound to arise. It's not at all uncommon to hear another cordless conversation on your phone or to hear the electronic pulse-beeping when you're not even dialing. Then there are cordless phone phreaks to deal with, who drive into heavily populated zones holding one of the common cordless models. It's called "cruising for dialtones." And some phones are nice enough to broadcast your conversation on an AM frequency. This feature isn't very good for private conversations. It helped shape a recent drug bust in the state of New York.

Recently, a lady in the Midwest called up her local electric company to tell them that she was going to be away for two months. A member of the 2600 Club heard this on his radio and, being in a good mood, called her and told her that important, personal business should *never* be discussed on cordless phones. After thanking him, she exclaimed, "That thing's going right back to the Phonecenter Store!"

1984 arrives in Hong Kong

The Los Angeles Times

In an effort to "discourage people from driving their cars in heavily congested areas" all 350,000 of Hong Kong's motor vehicles will be fitted with tracking devices that will let government computers know exactly where each car has traveled so that the owner can be billed for road use. This system could be in full implementation by 1987, if the government has its way. Such a system would also allow the police to quickly pinpoint the whereabouts of any vehicle. Tampering with the $45 tracking devices will be illegal and any attempt to do so will trigger street cameras to photograph the license plate of the car.

THE TRUTH BEHIND THOSE 9999 NUMBERS

by Mark Bluebox

Once upon a time, I was talking to one of my favorite friends, one of the nation's oldest and most experienced telephone enthusiasts—some might refer to him as a phone phreak. In this particular conversation, he mentioned to me that I might want to experiment with a series of 800 numbers: exchanges starting with 9, followed by the suffix 9999 (800-9xx-9999). And so I did, and a whole new world began to open up in front of me.

They were mostly weather and time numbers in various locations throughout the country. And, since these were 800 numbers, there was NO CHARGE! One number in particular was of a great deal of interest to me and to many others. This was 800-957-9999, which hooked up to WWV, the radio station operated by the National Bureau of Standards that does nothing but tell the time and give shortwave reports. This is the most accurate clock in the entire world! You either have to tune WWV in on a shortwave receiver or dial 303-499-7111 in Fort Collins, Colorado. Yet, here I was with an 800 access! Being a bit of a shortwave enthusiast, I don't have to tell you how convenient this was for me. Unfortunately, it got too convenient for too many people.

I guess I made the mistake of giving it to a former president of a large amateur radio club in the Dallas area. He, in turn, printed it in the Amateur Radio Newsbulletin where thousands of people probably saw it. Another statewide newsbulletin picked it up and printed it. Through an amateur radio news network which this bulletin was a part of, the news got as far as California.

One day, I called up the West Link Amateur Radio News Service at 213-768-7333. (This is a service located in West Link, California that broadcasts news over amateur radio, VHF, UHF, etc.) Their latest report had this little item: "Speaking of interesting things, the National Bureau of Standards has got a very convenient time number for those of you that are not constantly at a shortwave receiver. You can dial 1-800-957-9999 for WWV. It's just another good toll-free service for us to use." The avalanche had really begun now.

The West Link report was heard on bulletin stations all around the world and, apparently, one station in Nashville, Tennessee broadcast it. From there it fell into the hands of one of the writers for the DX program on Radio South Africa! I happened to be listening to a program where they were talking about pulling in distant time stations, weather stations, etc. He then mentioned, "For those of you that live in the United States, a convenient toll-free 800 number has been provided by the National Bureau of Standards for WWV and that number is 1-800-957-9999." Imagine my surprise! Once again, the number had been broadcast all around the world. People in many, many nations now had that number. Of course, the number only worked inside the United States, but the word was being spread by shortwave listeners and QSL people everywhere.

The number was getting swamped. Needless to say, it was busy much of the time. A government official, who *also* had this number, thinking that it was legitimate, called up WWV and complained. He told them that they needed to add some more lines to their new 800 number. The general manager of the station said, "I don't know *what* you're talking about. I don't know of any 800 number that gets you WWV."

The government official told him what the telephone number was. The general manager called it and heard his own station. Astounded, he contacted the Mountain Bell Telephone Company in Denver, Colorado. They said, "You're not paying for any 800 in-WATS number. We show 303-499-7111 for WWV, but we don't have any 800-957-9999."

Mountain Bell checked it out and sure enough, the number existed but not on *their* records. No one was getting charged for this! Now, of course, you know a monopoly as well as I do—they're *sure* not going to let anyone have a free ride. So they told the WATS coordinator to find out what happened. He finally made the discovery that some technicians had hooked that number up for transmission testing. [These switching technicians are toll technicians, AT&T Long Lines switching technicians, and carrier systems technicians. In other words, they're the group of people who link switching centers together, from New York to Los Angeles, for example. In this case, the whole escapade was a kind of group effort. The switchmen and the carrier people got together and set up this number for testing, finding noisy carriers, carriers with cross-talk on them, etc.]

The WATS coordinator told them they'd better get this number off—too many people knew about it. He told them to erase *every* 800 test line number that was on the system. Not surprisingly, someone also got chewed out very severely.

So, consequently, 800-957-9999 is no longer in existence. But since then, less than two weeks later, several of the 800 test numbers have begun to defiantly reappear. Check around, you'll probably find a few interesting ones. But I doubt if WWV's brief stint as a toll-free service will ever be repeated.

Ahoy, folks! If any of you have ever used an extender that goes by the name of 8006213129, you'd better give it a call now! The people running it have a message for you.

DISREGARD THIS: MTKIONS7752.4145.[illegible]

Position	Name	Extension
Office of the President		
The President	Ronald Reagan	2858
Special assistant	David C. Fischer	2168
Personal secretary to the President	Kathleen Osborne	2858
Office of the Counselor to the President		
Counselor to the President	Edwin Meese III	2235
Deputy counselor	James E. Jenkins	7600
Assistant counselor	Edwin W. Thomas Jr.	2235
Special assistant	Mitchell F. Stanley	2235
Assistant to the President for Cabinet affairs	Craig L. Fuller	2823
Secretary	Adela Gonzalez-Nardi	2823
Assistant director	T. Kenneth Gribb Jr.	2800
Administrative assistants	Karen Hart	2823
	Nancy A. (Missy) Hodapp	2800
Director of planning and evaluation	Richard S. Beal	6690
Office of Chief of Staff		
Chief of staff	James A. Baker III	6797
Executive assistant to the chief of staff	Margaret D. Tutwiler	6797
Staff assistant	Kathy Camalier	6797
Confidential secretary	Margaret Glasscock	6797
Deputy to the chief of staff	Richard G. Darman	2702
Administrative assistant	Sara Currence Emery	2702
Secretary	Janet F. McMinn	2702
Special assistant to the chief of staff	James W. Cicconi	2174
Presidential correspondence	Anne Higgins	7610
Special presidential messages	Dodie Livingston	2941
Office of the Deputy Chief of Staff		
Deputy chief of staff	Michael K. Deaver	6475
Assistant to the deputy chief of staff	Joseph W. Canzeri	2861
Staff assistant	Shirley Moore	6475
Special assistant to the President for private initiatives	James S. Rosebush	2957
Executive assistant	Bernyce Fletcher	2957
Director of special support services	Edward V. Hickey Jr.	2150
Deputy director of special support services	Dennis E. LeBlanc	2150
Deputy director of military office	Col. Frank E. Millner	2150
Army aide to the President	Lt. Col. Jose A. Muratti Jr.	2150
Air Force aide to the President	Maj. William M. Drennan	2150
Navy aide to the President	Cdr. William R. Schmidt	2150
Marine Corps aide to the President	Maj. John P. Kline Jr.	2150
Physician to the President	Dr. Daniel Ruge	2672
Director of advance	Stephen M. Studdert	7565
Deputy director of advance	Hugh L. O'Neill	7565
Administrative assistant	CeCe B. Kremer	7565
Trip desk officers	Marti J. Frucci	7565
	Karen Jones Roberts	7565
	Lynn Smallpage	7565
Advance staff	Robert K. Gubitosi	7565
	James F. Kuhn	7565
	Dan Morris	7565
	Lanny F. Wiles	7565
	Rocky D. Kuonen	7565
Director of scheduling	Gregory Newell	7560
Deputy director of scheduling	Tricia Rodgers	7560
Administrative assistant	Cristy Valentine	7560
Staff assistants	Michael Castine	7560
	Frances (Fan) Snodgrass	7560
	Netta A. Dickey	7560
Confidential assistant	Mary H. Rawlins	7560
President's diarist	Ellen Jones	7560
Appointments secretary	Helen C. Donaldson	7560
Staff directory for the First Lady	Peter McCoy	6702
Administrative assistant	Christine J. Hathaway	6702
Press secretary	Sheila P. Tate	7136
Assistant press secretary	Barbara Cook	7136
Personal secretary	Elaine Crispen	6633
Social secretary	Muffie Brandon	7064
Assistant social secretary	Linda Faulkner	7064
Scheduling director	Nina Wormser	7910
Special projects	Ann Wrobleski	7905
Office of the Vice President		
The Vice President	George Bush	7123
Executive assistant	Charles G. (Chase) Untermeyer	2587
Chief of staff	Daniel J. Murphy	6606
Deputy chief of staff	Richard N. Bond	7056
Military assistants	Lt. Col. Michael D. Fry	4213*
	Lt. Col. William Ecken	4223*
Counsel	C. Boyden Gray	7034
Deputy counsel	Rafael V. Capo	7034
Press secretary	Peter Teeley	6772
Deputy press secretary	Shirley M. Green	6772
Speechwriter	Christopher Buckley	7453
Domestic policy adviser	Thaddeus A. Garrett Jr.	2173
Assistant domestic policy adviser	Mary S. Gall	7935
National security affairs adviser	Nancy Bearg Dyke	4213
Congressional relations assistant	Robert V. Thompson	224-2424
Legislative assistant	Susan Alvarado	224-8391
Assistant for appointments and scheduling	Jennifer Fitzgerald	7870

All telephone numbers are on the 456- exchange except those marked with an asterisk, which are on the 395- exchange, and those listed in full.

Proper tabbing is extremely important when typing a list. Above is an example of tabs used successfully.

This here page is usually a continuation of page 5. However, when we get a blockbuster story like the one below, we have to reallocate our space. We know you'll understand. By the way, as long as we've got you looking up at this part of the page, why not take the time to send us some mail? Letters, articles, information, old telephones, paintings, anything, really. You know the address (it's on the front page). Let's hear from YOU.

FBI VS. HACKERS

(Continued from second page)

Telemail. They caused fits within Telemail when they decided to get a little bit cocky and see if they could shut down accounts and change passwords of the administrators and things like that. From there they have moved one step further to where they are now the same individuals communicating through the ADS systems and they also set up conference calls through the Bell System, so they're not just attacking one particular system or one individual avenue of communication — they try to hit them all. It's an ego trip for all of them.

Pen Registers

We would put a pen register on the phone line of the individual (suspect) and it would record only the digits dialed on his telephone — we would not use a full blown wiretap to record his voice. We can only put a pen register on an individual's phone for like, thirty days before we have to go back to a judge and try to get an extension and we try to minimize the use of our electronic surveillance equipment so the public does not think we're the Big Brother of 1984. (laughter) It's coming. Actually, we're already there! (hearty laughter)

We have not utilized any pen registers for the specific purposes of going after abusers of the ADS systems. First off, we have to have an actual case presented to us or a complaint. It's a roundabout way of doing it, but it's the way that we, in the bureau, have to have somebody outside come to us. Otherwise we can carry on the whole investigation without IBM even being aware that we are monitoring activity within their system and we don't want to become that secret police, or anything like that. We want to be above board and work with the corporations in the community.

Just How Much Trouble Are These Hackers In?

On the federal level we can prosecute them for telephone fraud (fraud by wire) if we can determine that the ADS is an ongoing business operation and that you are being denied your just revenues by them sneaking onto your system and abusing your system. The strictest penalty is a $1000 fine and 5 years in jail for an actual conviction of fraud by wire violation. Those are always lax — a more common sentence may be for an adult maybe a year in jail, 18 months, or a fine, sometimes they get probation, or agree to pay back any fraudulent money obtained or for services rendered or whatever to the client company — it stays on his record for a year, he's on probation for a year and at the end of that, his record is wiped clean. Rarely do they get the maximum penalty. It just doesn't happen.

Do Me a Favor

Please do not disclose any geographic location because we are kind of unique in that we do not have any other source available in any other part of the country that could supply us with information like this. He may be one of 200 people, but if you identify Michigan you identify between 2 or 3 individuals and it may burn the source.

We'd like to make it clear that we don't intend to do this kind of thing very often, since rumours about certain people being informants are very common in this business. But this is no rumour. This, friends, is solid fact — we would not have printed this story if we weren't able to substantiate the claims it makes, and we had no trouble at all doing that. Our intent in making this information known was not to screw up the FBI's fun (they're really not doing all that much out of the ordinary anyway), but rather to expose a very dangerous individual who goes by the name of Cable Pair (some say his real name is John Maxfield). This person has been posing as an extremely friendly hacker who lives in Detroit and is just bubbling over with technical information in exchange for your secrets. He claims to have been one of the nation's first phreaks, which may or may not be true. He gives out his telephone numbers freely, will do anything to communicate with somebody (like place conference calls from his own private PBX system, provided you give him YOUR phone number), and generally will use anything you say to him against you in the future. Our advise is simple: stay the hell away from this person. Even if you haven't done anything wrong yourself, your life can still be made miserable by him if you're even suspected of having contact with wrongdoers.

This latest turn of events has saddened us — we thought Cable Pair would be a promising contributor to this publication and instead we learned a valuable lesson: don't trust anybody. Have fun, Cable Pair. Enjoy yourself. Just don't expect to see any of us over at the Chestnut Tree Cafe with you. You're on your own now.

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/14/84

The following is a summary of trap and trace information received verbally from [redacted] b6 b7C b7E

[redacted]

[redacted] b7E

Investigation on 2/6/84 at Alexandria, Virginia File # Alexandria 196A-633 Sub E

by SA [redacted] DF:mb Date dictated 2/6/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7C
b7E

[redacted]

Review of [redacted]

b6
b7C
b7E

[redacted]

AX 196A-633

TABLE OF CONTENTS

REPORT FORMS (FD-302's)

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/10/84

This is a summary of the activities of [redacted] on GTE Telemail. b6 b7C

[redacted] used the names [redacted] and [redacted] on Telemail. [redacted] also routinely used the legitimate account registered as [redacted]. b6 b7C

[redacted] was a member of a group of illegal users called the "PHALSERS". [redacted] was registered as an illegal user in following companies: BMW, MARAVEN, TELENET, UAW and SCANNET. b6 b7C

[redacted] under one of his user names accessed the Telemail system on at least 247 different occasions between July 9, 1983, and October 12, 1983. Of those occasions, GTE Telemail captured 57 of his messages. b6 b7C

A fellow "PHALSER" has met [redacted] and can definitely identify [redacted] as [redacted] and [redacted]. [redacted] is described by this fellow PHALSER as the leader of the group and as a part-time volunteer at WUSB Radio Station, State University of New York at Stony Brook, Stony Brook, New York. b6 b7C

Information received from [redacted] b7E

[redacted]

[redacted] stated to this fellow PHALSER that he found out that the FBI was about to search for computer equipment at WUSB. [redacted] further told this person that he [redacted] was able to contact someone and get some material out of the room to be searched before the FBI searched it. A fellow radio station employee, [redacted], told the FBI that, at the time of the search, [redacted] gave instructions over the phone to [redacted] concerning b6 b7C

Investigation on 2/6/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted]:gaj Date dictated 2/6/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

the room to be searched. After the search, [redacted] thanked [redacted] for calling him and letting him know the room was going to be searched. The fellow PHALSER also said that [redacted] told him that he had given a statement to the attorney representing [redacted] admitting to his [redacted] use of Telemail. [redacted] also told the fellow PHALSER that "our story will be that I'm the only one who used Telemail." b6 b7C

On November 6, 1983, [redacted], using the legitimate account known as [redacted], left a message to the Public Relations Officer of GTE, stating that "we" represent PHALSE which is "an organization that has been rather active on the Telemail system over the past few months." In subsequent messages, [redacted] described the methods by which he and other PHALSERS penetrated the Telemail system and admits to reading the messages of legitimate companies (e.g. AMERICAN TELEPHONE AND TELEGRAPH messages). b6 b7C

Finally, [redacted] b7D b6 b7C

During the search of the WUSB Radio Station, two computer print-outs labelled "Telemail System Command Manual" dated September 20, 1983, were found. These are "bootleg" copies of system information that only a legitimate Telemail customer administrator should have access to. These print-outs were found in the same room from which [redacted], at [redacted] request, removed other material immediately before the search. b6 b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/13/83

[redacted], telephone number [redacted] advised he lives at this residence with [redacted] and [redacted]. b6 b7C

[redacted] said that he only used the Data System Terminal located in the bedroom of [redacted] in order to prepare a program which would [redacted]. b6 b7C

[redacted] advised he would rather not discuss the activities of [redacted] regarding his use of the computer equipment located in [redacted] bedroom. b6 b7C

[redacted] said he was born on [redacted] in [redacted] telephone [redacted]. b6 b7C

Investigation on 10/13/83 at [redacted] File # BO196B-2942

by SAS [redacted] and [redacted] JKE/mtm Date dictated 10/13/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/28/83

[redacted], telephone [redacted], was telephonically contacted on December 20, 1983. b6 b7C

[redacted] said he had spoken to various "friends" and based on their advice he had decided he did not want to talk to the Federal Bureau of Investigation (FBI) at this time.

Investigation on 12/20/83 at Hauppauge, New York (Telephonic) File # Alexandria 196A-633 Sub E

by SA [redacted] /btd Date dictated 12/21/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/28/83

telephone [redacted], was contacted by Special Agent (SA) [redacted] telephonically from the Hauppauge, New York, Resident Agency of the Federal Bureau of Investigation (FBI). [redacted] was told that the FBI would like to interview him concerning statements made to him by [redacted] on the telephone on October 13, 1983, at the time of an FBI search of the WUSB Radio Station on the State University of New York at Stony Brook. b6 b7C

[redacted] first stated he knew nothing about the incident. He was then told that the FBI had information that [redacted] had asked [redacted] to go to the room where the computers were stored and remove certain materials before the agents could get to them. [redacted] was further told that this removal of items by him might constitute obstruction of justice. b6 b7C

[redacted] said that he wanted to talk to an attorney and [redacted] agreed to have his attorney call SA [redacted] at the Hauppauge, New York, Resident Agency. b6 b7C

(Telephonic)

Investigation on 12/20/83 at Hauppauge, New York File # Alexandria 196A-633 Sub E

by SA [redacted] /btd Date dictated 12/21/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

11/18/83

Date of transcription

[redacted] called the Alexandria Office of the Federal Bureau of Investigation (FBI) on this date and requested to speak to Special Agent (SA) [redacted]. [redacted] was advised of his rights orally and he thereafter indicated that he still wanted to talk with this agent concerning his involvement in the illegal accessing of the GTE Telemail system.

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

Investigation on 10/19/83 at Alexandria, Virginia File # Alexandria 196A-63

by SA [redacted]:gaj Date dictated 10/21/83

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 11/18/83

[redacted] called the Alexandria Office of the Federal Bureau of Investigation (FBI) on this date and requested to speak with Special Agent (SA) [redacted]. b6 b7C b7D

This agent advised [redacted] of his right to remain silent and [redacted] indicated that he was aware of his rights, but still wished to talk with this agent concerning illegal accessing of GTE Telemail system. b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

Investigation on 10/27/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 10/28/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/14/83

[redacted](protect identity), telephonically contacted the Alexandria Office of the Federal Bureau of Investigation (FBI), and thereafter provided the following information: b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] provided the following information:

1) [redacted] b6 b7C b7D

2) [redacted] b6 b7C b7D

Investigation on 12/6/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] /DF:mb Date dictated 12/6/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/16/84

[redacted] telephonically contacted this agent and thereafter provided the following information:

b6
b7C
b7D

His date of birth is [redacted] and his Social Security Account Number is [redacted] His home address is [redacted] also provided this information:

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

Investigation on 1/11/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted] gaj Date dictated 1/11/84

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/25/84

[redacted], home phone [redacted] or [redacted], telephonically contacted this agent on this date. [redacted] thereafter provided the following information:

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

Investigation on 1/23/84 at Alexandria, VA File # Alexandria 196A-633

by Sa [redacted]mbe Date dictated 1/23/84

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 12/28/83

telephone [redacted], was advised of the official identities of the interviewing agents and thereafter provided the following information: b6 b7C

He is [redacted]

[redacted] is well known at the WUSB Radio Station and is considered to be a "phone expert." During the summer of 1983, [redacted] saw a handwritten note on a bulletin board at the radio station that said something to the effect of "the phone police are coming." At one point, [redacted] and [redacted] were standing next to the bulletin board and [redacted] asked [redacted] what that sign meant. [redacted] replied something to the effect of, "I don't want to talk about it." [redacted] felt that [redacted] was continuously doing something with the phones that he did not want other people to know about. b6 b7C

[redacted] also has personal knowledge that [redacted] uses the telephone "constantly" to make various types of telephone calls to 800 numbers and is much more knowledgeable about unusual features of the telephones than other people. b6 b7C

In approximately May or June, 1983, [redacted] saw [redacted] call some sort of answering service or message service on the telephone. [redacted] was using the telephone in the radio station and the phone was on a speaker at the time. [redacted] saw [redacted] punch various buttons on a touch-tone telephone and then a voice would say something to the effect, "Press one to leave a message, two to hear a message, etc." When [redacted] saw that [redacted] and others had heard this, he seemed to be very concerned. At this same time, [redacted] also heard a message from [redacted] to [redacted] being delivered over this message system. [redacted] clearly recognized [redacted] voice and [redacted] knows that [redacted] and [redacted] are good friends. It is clear to [redacted] that the message being delivered on the telephone system was from [redacted] to [redacted] b6 b7C

[redacted] said that [redacted] specifically called the "message service" to check for his messages. [redacted] was also present when this happened. b6 b7C

Investigation on 12/20/83 at [redacted] File # Alexandria 196A-633 Sub E

by SAs [redacted] & [redacted] Date dictated 12/21/83 b6 b7C

DF/btd

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

According to [redacted] has moved somewhere to upstate New York. He moved in August, 1983. [redacted] has visited [redacted] within the past week. b6 b7C

In approximately May, 1983, [redacted] saw [redacted] and [redacted] and [redacted] (Last Name Unknown) at a pay telephone in the Student Union at the State University of New York Campus at Stony Brook. [redacted] watched as [redacted] dialed a number and [redacted] said, "I'm calling the Defense Department." [redacted] then said that the number rang a couple of times and then he would receive a dial tone. b6 b7C

On October 13, 1983, the day the premises of WUSB Radio Station were searched by agents of the FBI, [redacted] was present when agents first came to the station and he indicated they had a search warrant. At this point, [redacted] called [redacted] to report that the agents were there because he thought the computer in the station belonged to [redacted] called [redacted] and said something to the effect of, "The phone police are here." [redacted] appeared very disturbed and asked [redacted] what he meant. [redacted] said, "The FBI is here and they have a search warrant for computers." [redacted] replied something to the effect of, "Thanks for letting me know. There is something we have to get rid of or there is something we have to do." [redacted] also asked [redacted] to find out if anyone was down in the room where the computer was. [redacted] reported that [redacted] was, in fact, in that room and [redacted] asked [redacted] to call [redacted] to the telephone. [redacted] did call [redacted] to the telephone and [redacted] listened as [redacted] seemed to be getting some sort of instructions from [redacted] then left and apparently went back to the room where the computer was. [redacted] says he clearly got the impression that [redacted] was asking [redacted] to remove something from the room where the computer was. b6 b7C

After the search, [redacted] came back to [redacted] and said, "Thank you for calling me, it was important that you did that." [redacted] again felt that [redacted] had succeeded in having [redacted] get material out of the room to be searched before the FBI agents found it. b6 b7C

FD-517 (12-2-77)

FEDERAL BUREAU OF INVESTIGATION

PROSECUTIVE REPORT OF INVESTIGATION CONCERNING

[redacted]
also known as [redacted]
also known as [redacted]
also known as [redacted]
also known as [redacted]
also known as [redacted]
also known as [redacted]
FRAUD BY WIRE; CONSPIRACY

b6
b7C

Copy to: 1 - USA, Alexandria, Va.
(Attn: AUSA [redacted])

b6
b7C

FBI/DOJ

AX 196A-633

TABLE OF CONTENTS

AX 196A-633

NAMES OF DEFENDANTS:

1. [redacted], described as:

Race
Sex
Date of Birth
Height
Weight
Eyes
Iowa Motor
Vehicle Number
Address

[redacted] yrs old

b6
b7C

~~C-1~~

AX 196A-633

2. [redacted], described as:

Race
Sex
Date of Birth
Height
Weight
Social Security
Account Number
Address

[redacted] [redacted] yrs old

[redacted]

b6
b7C

AX 196A-633

3. [redacted], described as:

Race
Sex
Date of Birth
Place of Birth
Social Security
Account Number
Address

[redacted] yrs old

b6
b7C

AX 196A-633

4. [redacted], described as:

Race [redacted]
Sex [redacted] yrs old
Date of Birth
Social Security
Account Number [redacted]
Address [redacted]

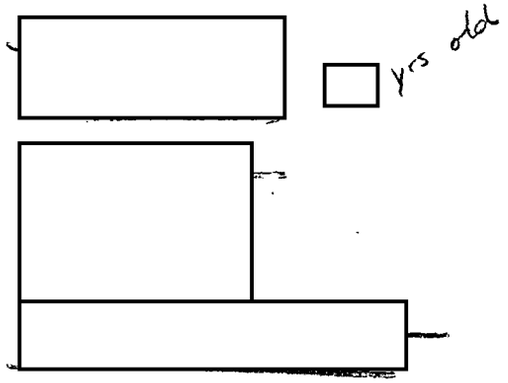
Present Address [redacted]

b6
b7C

AX 196A-633

5. [redacted], described as:

Race
Sex
Date of Birth
Social Security
Account Number
Height
Weight
Eyes
Hair
Address



b6
b7C

AX 196A-633

6. [redacted], described as:

Race [redacted]
Sex [redacted]
Date of Birth [redacted] [redacted] yrs old
Social Security Account Number [redacted] (provided by subject)
[redacted] (from NCIC)

b6
b7C

Height
Weight
Eyes
Hair
Place of Birth
Address [redacted]

C-6

AX 196A-633

PROSECUTIVE STATUS:

1. On August 30, 1983, the available facts in this matter were presented to Elsie Munsell, United States Attorney, Eastern District of Virginia, who advised she would consider prosecution in the matter.

2. On October 12, 1983, the premises located at (1) [redacted]; (2) [redacted]; and (3) [redacted] were searched pursuant to a duly authorized federal search warrant and various computer paraphenalia were seized. b6 b7C

3. On October 13, 1983, the premises located at [redacted] was searched pursuant to a duly authorized federal search warrant and various computer paraphenalia were seized. b6 b7C

~~D 1~~

AX 196A-633

WITNESSES:

1. [redacted]
GTE Telemail
8229 Boone Boulevard
Vienna, Virginia
Telephone [redacted]

b6
b7C

Can provide details of GTE Telemail operations, methods of detecting unauthorized users and procedures for obtaining print-outs of customer messages.

2. [redacted]
Special Agent
Federal Bureau of Investigation

b6
b7C

Can supply details of investigation.

3. [redacted]
Special Agent
Federal Bureau of Investigation
Omaha

b6
b7C

Can supply details concerning search of [redacted]

4. [redacted]
Special Agent
Federal Bureau of Investigation
Tucson

b6
b7C

Can supply details concerning search of [redacted]

5. [redacted]
Special Agent
Federal Bureau of Investigation
San Diego

b6
b7C

Can supply details concerning search of [redacted]

AX 196A-633

6. [redacted]
Special Agent
Federal Bureau of Investigation
Albany

b6
b7C

Can supply details concerning search of [redacted]

~~E-2~~

AX 196A-633

EVIDENCE:

RE: [redacted]

1. Summary of seven messages left on GTE Telemail by [redacted] (original in possession of [redacted], GTE Telemail [redacted]). b6 b7C

2. Summary of 53 items of relevance seized during search (in possession of FBI Alexandria).

3. Summary of information retrieved from floppy discs (discs in possession of FBI Alexandria).

4. Summary of trap and trace information received from [redacted] (original in possession of FBI Alexandria). b7E

5. List of charges attributable to [redacted], aka [redacted] (original in possession of [redacted]). b6 b7C

6. FD-302 with attached list of items seized in search.

7. Two index cards, seized in search of [redacted], aka [redacted]. One contains the name [redacted], followed by the phone number [redacted] (W) and [redacted] (H). The other card contains the number [redacted], followed by the name [redacted] (originals in posssesion of FBI Alexandria). b6 b7C

RE: [redacted]

1. Summary of 12 messages left on GTE Telemail by [redacted] (originals in possession of [redacted]). b6 b7C

2. Summary of 11 items of evidence of relevance seized during search (in possession of FBI Alexandria).

3. Summary of information retrieved from floppy discs (discs in possession of FBI Alexandria).

4. List of charges attributable to [redacted], aka [redacted]. b6 b7C

PI

AX 196A-633

RE: [redacted]

b6
b7C

1. Summary of 62 messages left on GTE Telemail by [redacted] (originals in possession of [redacted]).

2. Summary of ten items of relevance seized during search (in possession of FBI Alexandria).

3. List of charges attributable to [redacted], aka [redacted] (in possession of [redacted]).

b6
b7C

RE: [redacted]

b6
b7C

1. Summary of 40 messages left on GTE Telemail by [redacted] (originals in possession of [redacted]).

2. Summary of ten items of relevance seized during search (in possession of FBI Alexandria).

3. Copy of trap and trace information provided by [redacted] (original in possession of FBI Alexandria).

b7E

4. List of charges attributable to [redacted], aka [redacted] and [redacted] (original in possession of [redacted]).

b6
b7C

RE: [redacted]

b6
b7C

1. Summary of four messages left on GTE Telemail by [redacted] (originals with [redacted]).

2. Copy of first sheet of a list of names seized from [redacted], aka [redacted], bearing the listing [redacted] (original with FBI Alexandria).

b6
b7C

3. List of charges attributable to [redacted], aka [redacted] (original with [redacted]).

b6
b7C

RE: [redacted]

b6
b7C

1. Summary of six messages left on GTE Telemail by [redacted] (originals with [redacted]).

2. Copy of first sheet of a list of names seized from [redacted] bearing the listing [redacted] (original with FBI).

b6
b7C

AX 196A-633

3. Letter with enclosure sent to FBI Alexandria, dated January 14, 1984, by [redacted]. b6 b7C

4. Letter sent to FBI Alexandria by [redacted], dated January 26, 1984. b6 b7C

5. List of charges attributable to [redacted], aka [redacted] (original with [redacted]). b6 b7C

~~F-3~~

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/15/83

The following is a summary of messages left by the illegal user using the name [redacted] on GTE Telemail. b6 b7C

The date and time of each message is provided with a synopsis of particularly significant messages included.

1) August 30, 1983, 1:06 p.m. (All times Eastern Daylight Time)
2) September 1, 1983, 8:44 p.m.
3) September 6, 1983, 12:58 a.m. This message is to [redacted], and the text is as follows: "Hi [redacted], if you get the chance would you please send the programs we discussed?" b6 b7C
4) September 23, 1983, 9:09 p.m. Message reads, "Hi [redacted]..welcome to Telemail. Let me know how you like it." b6 b7C
5) September 23, 1983, 9:26 p.m. Message reads, "Welcome to Telemail. Hope that you enjoy the system. If you want to send any info, type A at action. Type exit and you will get the command prompt. There are extensive help commands. Later, [redacted] b6 b7C
6) September 25, 1983, 11:01 a.m. Message reads, "Welcome to the company. See you at the security seminar in September."
7) October 11, 1983, 12:18 a.m. Message reads, "Welcome to the services. If I may be of further services please let me know."

Investigation on 12/9/83 at Alexandria, Virginia File # Alexandria 196A-633 (SUB T)

by SA [redacted]:btl Date dictated 12/9/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/21/83

The following is a summary of a review of evidence seized in the search of the residence of [redacted], [redacted]. The following articles with relevence to this investigation were found: b6 b7C

1.) A photocopy of a page from the publication "80 Micro-Computing", dated March, 1981, with the telephone number 1-402-741-7733 followed by the words Telenet local access number. This is followed by the words @ mail, password = phones, user = phones.

2.) Hand-written note in a red notebook as follows: [redacted]. b6 b7C

3.) An envelope with the hand-written words: Silver Box followed by the letter A-697-1633, B-770-1633, C-852-1633, D-941-1633. This is followed by the words Blue Box and the number 2600.

4.) A brown scrap paper with the words "Admin Hack" followed by the words "Admin/Prime Computer".

5.) A blue sheet of paper with numerous 800 Modem numbers on it and approximately 20 "Wats extenders". This sheet of paper also has the words "source online lists users". This is followed by the number [redacted] and the words Delta Comm. This is followed by the number [redacted] and the word Kremlin. b6 b7C

6.) Computer print-out with a message from [redacted] on how to hack Telenet. The hand-written words "try Telenet-212 99 are found on this print-out. b6 b7C

7.) Print-out with hand-written words "AHSC". AHSC is American Hospital Supply Corporation and this was one of the companies that was most often penetrated by hackers in telemail.

8.) Print-out of a computer program to search for computer numbers.

Investigation on 11/7/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 11/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

9.) Print-out with messages from TDK (on hacking Sprint codes), and others including [redacted] on illegally accessing Autovon, using blue boxes, and various Telenet accounts and passwords. b6 b7C

10.) Print-out of a program to search for MCI telephone access codes.

11.) A program to automatically dial various phone numbers, including those for Metrophone access codes and MCI access codes.

12.) A print-out with a message from [redacted] listing "dialups" for the National Institute of Health Computers. This print-out also contains a message from [redacted] wherein he offers a Sprint code hacking program and "valid Sprint codes". b6 b7C

13.) A print-out of Edunet file names.

14.) A print-out of a message from [redacted] listing various computers and connect addresses. There is also a message from [redacted] about a blue box. b6 b7C

15.) A print-out from the Osuny bulletin board with information about how to rig your phone for a long distance dialing without being charged. This print-out also contains Metrophone access numbers. It also contains a message from [redacted] wherein he claims to have 70 source accounts. There is also a message from Mandrake concerning the phone company's detection of hackers. b6 b7C

16.) A print-out about phone phreaking.

17.) A print-out with messages from [redacted] with connect addresses of Arpanet hosts. This print-out also contains messages from [redacted] and [redacted] listing Telenet accounts. b6 b7C

18.) A computer print-out of a program to search for computer numbers.

19.) A print-out with a message from [redacted] listing Metrophone access numbers. b6 b7C

20.) A print-out of a program for an automatic telephone dialer to get MCI or Sprint access codes.

21.) A print-out from the Security Land bulletin board with a message from [redacted] giving "Mainframe" numbers and passwords. This message also contains information on Arpanet. b6 b7C

22.) This is a print-out containing Metrophone access codes left by [redacted] is [redacted], whose residence at [redacted] was searched on October 12, 1983. b6 b7C

23.) A print-out containing a program designed to search for computer access numbers.

24.) A print-out of a program designed to search for computer access numbers.

25.) A print-out containing information on how to access Telenet, with a message from a hacker known as [redacted]. This print-out also contains a message from [redacted] containing Sprint codes, MCI codes and Metrophone codes. b6 b7C

26.) A print-out of a type-written paper titled "Cheating power companies, vending machines, etc."

27.) A print-out with information on how to alter your phone to manufacture blue boxes and other devices to cheat the phone company.

28.) A print-out with Telenet access numbers and connect addresses, including "Citibank Cash Manager" and "Nasa Recon".

29.) A print-out with a message from [redacted] (aka [redacted]) and [redacted], both of which offer 800 numbers that can be extended to call anywhere in the United States and MCI access codes. The message from [redacted] gives the number [redacted] as a contact number for his Modem. b6 b7C

30.) A photocopy of an MCI credit card issued to [redacted]. It lists customer service number 612-544-8171 and bears account number [redacted]. b6 b7C

31.) A print-out with numerous Satelco access codes.

32.) A print-out with numerous Telenet connect addresses.

33.) A paper with various 800 numbers written on it.

34.) A print-out with a message in reference to the password to the Boystown PDP-11 Computer.

35.) A print-out with Compuserve and Source accounts listed. This print-out also lists access code numbers for overseas long distance lines.

36.) A print-out from the "Pirates Palace Bulletin Board" and it lists numerous Sprint codes, Telenet hosts and connect addresses, many of which bear hand-written notations such as "O.K.", "No good", etc.

37.) A print-out concerning "Autonet access lists".

38.) A print-out listing "ADP Autonet Extended United States Access Locations".

39.) A print-out with a list of various bulletin boards and phone numbers.

40.) A print-out with a list of numerous Sprint access numbers.

41.) A print-out of a list of "Pirate Bulletin Boards".

42.) A print-out with 800 numbers and extender codes, Sprint codes, MCI codes, and Metrophone codes. This print-out also contains password for a source account. This print-out also contains a message describing "phreaking" as a felony and stating that sharing information on these bulletin boards is "aiding and abetting".

43.) A print-out referring to the arrest of a hacker known as [redacted] by the Los Angeles Police Department. b6 b7C

44.) A print-out with ITT access codes. It also contains numerous MCI and Sprint codes.

45.) A print-out of numerous Telenet hosts and connect addresses.

46.) A print-out of a computer program designed to search for other computer numbers.

47.) A print-out of bulletin boards and access numbers.

48.) A piece of blue paper with a Compuserve account number, ID number and password. This blue paper also contains a source connect address, user name and password.

49.) Another sheet of blue paper with a source identification name and password.

50.) A copy of an MCI bill to [redacted] b6 b7C

51.) A print-out with numerous Sprint codes and access numbers.

52.) A print-out with numerous Sprint codes and access numbers, many with hand-written notations such as "N. G." and "Check".

53.) A print-out with numerous Metrophone access codes.

~~E9~~

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/30/84

On October 12, 1983, a search pursuant to a Federal Search Warrant was executed at the home of [redacted] b6 b7C

The "floppy discs" that were seized in this search were examined by [redacted], a computer programmer. The following is a summary of [redacted] findings concerning information on these floppy discs: b6 b7C

On the disc labelled 196-633 Sub T, 1B1, Item Number 9, Number One, a program called, "Code Breaker for the Hayes Smartmodem" by [redacted] was found. This is a program designed to find access codes for MCI or some similar long distance communication service. A program called "MCI Hacker" is designed specifically for finding MCI authorization codes. A program called "MCI FIND" is a list of access codes actually found by a computer. This was probably produced by the program called "MCI Hacker." b6 b7C

On the disc labelled 196-633 Sub T, 1B1, Item Number 9, Number Two, a program called "C-SCAN" was found. This is a program which searches for other computers via the telephone. A program called "CODE/CHK" is designed to search for authorization codes for long distance communication services. This program contains this "you are now running one of the most powerful computer programs to search for a correct authorization code on many of the different companies that provide long distance communication services. Use of this program may be against many different laws."

On the disc labelled 196-633 Sub T, 1B1, Item Number 9, Number Three, had a program called "MNET/OMT" was found. In this program appears to be a compuserve account number. A program called "SOURCE/OMT" appears to contain a source account number.

Investigation on 1/13/84 at Alexandria, Virginia File # Alexandria 196A-633 SubT

by SA [redacted] :mbe Date dictated 1/13/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

On the disc labelled 196-633 Sub T, 1B1, Item Number 9, Number Four, was found a program labelled "MCI." This program is designed to obtain MCI authorization codes. A program entitled "COMFAST" by [redacted], subroutines, by [redacted], is designed to search for other computers via the phone. A program called "SMFIND" is designed to obtain MCI authorization codes and was designed by [redacted]. b6 b7C

On the disc labelled 196-633 Sub T, 1B1, Item Number 9, Number Five, appears a message from a hacker promising information on how to break in to a computer called RSTS.

On the disc labelled 196-633 Sub T, 1B1, Item Number 9, Number Six, is the program called "PAMS." This is a listing of other phone numbers connected to computers.

On the disc labelled 196-633 Sub T, 1B1, Item Number 9, Number Seven, appears the program called "TELENET." This is a list of numerous "connect addresses" for Telenet computers. A program called "DIAL" is designed to dial a telephone number entered into the keyboard and then searched for numbers.

On the disc labelled 196-633 (T), 1B1, Iitem Number 9, Number Eight, also labelled "Auto Dial Hack" is found a basic program that checks for authorization codes.

On the disc labelled 196-633 (T), 1B1, Item Number 9, Number Nine, is found a program called "DIAL" in which there is an automatic phone dialing program that mentions telenet.

On the disc labelled 196-633 (T), 1B1, Item Number 9, Number Ten, is a program labelled "TELECOM." This program contains assorted modem control programs.

On the disc labelled 196-633 (T), 1B1, Item Number 9, Number Eleven, is found a program labelled "TERM MASTER." This disc contains sorted programs to control modem dialing.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 1/30/84

This report reflects a review of trap and trace information and [redacted] pursuant to a Federal Grand Jury subpoena for [redacted] b3 b7E

Review of [redacted] b3 b7E

Review of [redacted] b3

revealed the following:

[redacted] b3 b7E

[redacted] b3 b7E

[redacted] b3 b7E

Investigation on 1/26/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 1/26/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~F12~~ 43

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS	
[redacted]	AHSC	$62.29	July, August, September	
	UAW	$31.00	September	
[redacted]	Maraven	$16.00	August, September	b6 b7C
	Telenet	$108.00	July, August	
[redacted]	BMW	$0.29	September	
		$127.58		
[redacted]	CBOT	$2.00	September	
[redacted]	RADA	$1.00	September	b6 b7C
		$3.00		
[redacted]	Maraven	$24.00	August	
	Telenet	$325.00	July	b6 b7C
	Telenet	$151.00	August	

SUBT [redacted]

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F23 54

FD-302 (REV. 3-8-77

44-CC file

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 10/19/83

At approximately 8:10 a.m. on October 12, 1983, a search warrant was executed on the premises known as [redacted], [redacted]. The following Special Agents (SAs) of the Federal Bureau of Investigation (FBI) were present during the search which concluded at 10:30 a.m. this date: b6 b7C

[redacted] b6 b7C

The attached schedule lists all items of an evidentiary value which were seized. All items seized with the exception of Item #18 were located in the southwest bedroom/office of the residence by SA [redacted] (VLB). Item #18 was found by SA [redacted] (DLH) in the master bedroom. The inventory itself was prepared by SA [redacted] (RGC). b6 b7C

Investigation on 10/12/83 at [redacted] File # Omaha 196A-922

by SA [redacted] SA [redacted] SA [redacted] SA [redacted] SA [redacted] SA [redacted] b6 b7C

Date dictated 10/18/83

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F28 59

This is to certify that on October 12, 1983 at 8:15 AM, Special Agents of the Federal Bureau of Investigation, U. S. Department of Justice, at the time of conducting a search of my person and/or the premises at [redacted] b6 b7C obtained the attached listed items. I further certify that the listed items represent all that was obtained by Special Agents of the Federal Bureau of Investigation, U. S. Department of Justice.

Signed _____

Witnessed [redacted] b6 b7C
Special Agent
Federal Bureau of Investigation
U. S. Department of Justice

Witnessed [redacted] b6 b7C
Special Agent
Federal Bureau of Investigation
U. S. Department of Justice

~~F29~~

SEARCH INVENTORY/RECEIPT

DATE: 10/12/83

TIME: 8:30AM

LOCATION: [ ] [ ] b6 b7C

ITEM #	ITEM DESCRIPTION	WHERE FOUND	FOUND BY
1.	Radio Shack TRS-80 Model III Video Terminal and associated wiring	dept - S.W. Bedroom Office	VLB
2.	Radio Shack TRS-80 Keyboard S.N. 014408	S.W. Bedroom	VLB
3.	Radio Shack TRS-80 Line Printer Model 737-1 SN 5727	S.W. Bedroom	VLB
4.	Radio Shack TRS-80 Video Display SN 22331	S.W. Bedroom	VLB
5.	Radio Shack TRS-80 Expansion Interface SN 02530 Dept of Baltimore Public Schools Baltimore West High #81246	S.W. Bedroom	VLB
6.	Radio Shack TRS-80 Mini Disk SN 23542-1 Dept of Baltimore Public Schools Baltimore West High #81246	S.W. Bedroom	VLB
6.A	Terry Master Label on black desk unit as #6	S.W. Bedroom	VLB
7.	Silver box similar to item 6. Label Drive 1	S.W. Bedroom	VLB
7A	Black disk - label illegible (PH)	E-30 61	

SEARCH INVENTORY/RECEIPT

DATE: 10/12/93

TIME: 9:15 AM

LOCATION: [redacted] [redacted] b6 b7C

ITEM #	ITEM DESCRIPTION	WHERE FOUND	FOUND BY
8.	Quattro Power Strip	S.W. Bedroom Office	VLB
9.	Radio Shack TRS-80 Direct Fdi Box w/37 disks	S.W. Bedroom "	VLB
10.	Radio Shack TRS-80 Serial Interface 1CC4953	S.W. Bedroom "	VLB
11	2 Radio Shack TRS-80 Disc Operating Manuals & Basic Programming Manuals w/ Cassette	S.W. Bedroom "	VLB
12.	Black 3-ring book "Pallidas" w/ address	S.W. Bedroom "	VLB
13	Radio Shack TRS-80 Manual re-Memory Program	S.W. Bedroom "	VLB
14.	Radio Shack TRS-80 Manual Tape Media last 26-1563 w/17 diskettes	S.W. Bedroom "	VLB
15.	Brown Address Book computerized 3"x2"	S.W. Bedroom "	VLB
16	BASIC Book - Misc note pages 1-330-336	S.W. Bedroom "	VLB
17	Loose Pack misc contain misc papers.	S.W. Bedroom "	VLB
18.	Misc Papers - computer sheets	Client Master Bedroom	DLH
19.	Black Memo Notepad w/misc	Desk - S.W. Bedroom	VLB

62

SEARCH INVENTORY/RECEIPT

DATE: 10/12/83
TIME: 9:56 AM
LOCATION: [redacted] [redacted] b6 b7C

ITEM #	ITEM DESCRIPTION	WHERE FOUND	FOUND BY
20.	Box of 15 Diskettes	3N Bedroom Office	VLB
21.	Kaypro "Extra" Modem Telex	3N " "	VLB
22.	Misc computer parts	3N " "	VLB
23.	Smartmodem 300 Copy Kit Model 96-196 Tape/Slack	3N " "	VLB
23A	Manual for item 23	3N " "	VLB

FBI 63

Page 3 of 3 Pages

FD-302 (REV. 3-8-77

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 10/18/83

At approximately 6:15 p.m. on October 11, 1983, Special Agent (SA) [redacted], Federal Bureau of Investigation (FBI), presented an affidavit in support of a search warrant to United States (U.S.) Magistrate Richard W. Peterson, Council Bluffs, Iowa. This affidavit had previously been authorized by Assistant United States Attorney (AUSA) [redacted], Southern District of Iowa (SDI), Des Moines, Iowa. U.S. Magistrate Peterson approved the search warrant for search of the premises known as [redacted]

b6
b7C

The warrant was executed at 8:10 a.m. on October 12, 1983, by the following Special Agents of the FBI, Omaha, Nebraska:

[redacted]

b6
b7C

The search was completed at 10:30 a.m. A copy of the search warrant and items seized was left at the premises since no occupants were present. It should be noted the side door to the residence was left open and access to the house was made through this entrance. Efforts to locate the owner of the residence were negative. Pottawattamie Sheriff was notified of the search warrant. General condition of the house was that it was in complete disarray.

Three telephones were located in the residence with numbers as follows:

Location	Number
Southwest Bedroom	[redacted]
Master Bedroom	[redacted]

b6
b7C

196A-633 46

Investigation on 10/11-14/83 at [redacted] File # Omaha 196A-922

b6
b7C

by SA [redacted] :emb Date dictated 10/17/83

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~F33~~ 64

Kitchen [redacted] b6 b7C

The search warrant was returned to U.S. Magistrate Peterson at 10:15 a.m., October 14, 1983, at Suite 406, First Federal Savings and Loan Building, Council Bluffs, Iowa.

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 1/4/84

The following is a summary of messages left by the illegal user using the name [redacted] on GTE Telemail. b6 b7C

The date and time of each message is provided, with a synopsis of particularly significant messages included:

1. July 26, 1983, 6:04 a.m. (All times are Eastern Daylight Time)

2. July 26, 1983, 1:55 p.m. (Mountain Day Light Time) This message is from [redacted] to Phalse and the subject is "The first atomic bomb explosion). This message is an extremely long message that purports to be a true story told to [redacted] by Laura Fermi, widow of the nuclear physicist, Enrico Fermi. This message mentioned "We lived in Hyde Park which is a suburb of Chicago." b6 b7C

3. August 3, 1983, 4:28 p.m. This message inquires about an ADS System in Chicago.

4. August 5, 1983, 2:48 p.m. This message is in reference to publication of the 2600 Magazine.

5. August 8, 1983, 12:26 p.m. This message states in part "I got a phone call here at home Sunday morning from the Sysop of Osuny. This message also indicates that the Sysop of Osuny spoke with [redacted] on the phone." It appears that The Sysop of Osuny may have the home phone numbers for both [redacted], aka [redacted] and [redacted]. b6 b7C

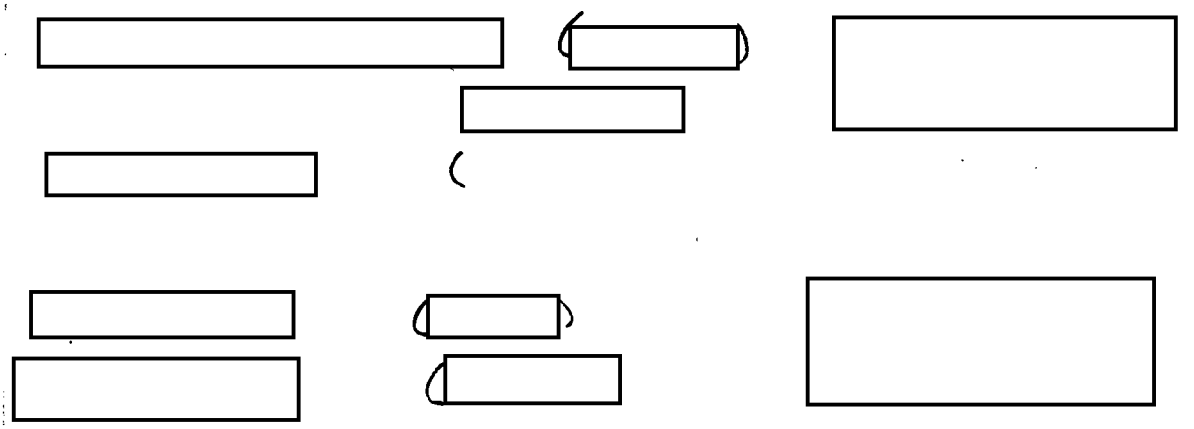
6. August 9, 1983, 12:22 a.m. This is another message concerning a phone call from the Sysop of Osuny.

Investigation on 12/8/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:gkh Date dictated 12/83/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~F35~~ 66



b6
b7C

[redacted]

Phone [redacted]

b6
b7C

January 26, 1983

[redacted]
Federal Bureau of Investigation
300 North Lee Street - Room 500
Alexandria, VA 22314

b6
b7C

Dear [redacted]:

This letter is in reference to your various phone calls to me regarding the investigation you are conducting. I was happy to speak with you, and I gave you all the information I have available, which was very little. When you have called, you have kept insisting that there was something I knew further about the case.

You have allueded to various coincidences which seem to convince you that I am the [redacted] you seek. Today you suggested I was also [redacted]. I would simply like to point out that you had no comparisons to draw at all until you called me the first time and I voluntarily told you much about myself.

b6
b7C

Because I do volunteer work for the library at the radio station called CRIS (Chicago Radio Information Service) you found a connection to [redacted]. Because some freak picked up on my BBS phone line several months ago, and then disseminated my number to his friends to hassle me, you found a connection to [redacted].

b6
b7C

When you first called me, you did not even have my correct name, and you asked for "R. Benedict" which was my deceased godmother's name, a fine older lady who lived here for many years. I told you my name, and I gave you what information I could. I told you that if there was one call for [redacted] there were fifty of them over the course of the summer. In each and every case I told the caller, "SORRY, WRONG NUMBER." I told you of one such caller who called 2-3-4 times from Texas (he said) who asked for [redacted] [redacted] new number, etc. I told you this person had some terrible sound in his nose all the time he talked. I think I also told you that when I first started my [redacted] BBS, it got trashed something awful by the same person(s) unknown.

b6
b7C

76

 b6 b7C

You pointed out a coincidence along the way that on one of the IBM systems in your investigation some person used the password [redacted]. I do not know what to make of this, and while I might agree that there are various things you mentioned which have similarities to my own life, I simply cannot and will not assume responsibility for anything someone does that happens to look like something about me. b6 b7C

Now, just by coincidence of course, two days after you spoke to me the first time, I got a piece of mail for your [redacted]. It did not even have the correct address/apartment number (we have no such number as whatever it said). I forwarded this to you without hesitation - unopened - if it would help you. I added a note saying that of all the times there had been attempts to contact this person, it was the first time someone had bothered to write. I have attempted to be cordial in our phone conversations, but I do not like your repeated insinuations that I will be in alot of trouble, be forced to come all the way to Virginia, etc. I have never hesitated to talk to you, even though on both occassions that you called me I had just gone to bed from an overnight work shift. b6 b7C

You are free to tap my phone and dont need my permission. You are free to compile all my phone records. If you think you can uncover some big secret out here you are welcome to have someone come and visit. Don't even tell me - just surpirse me at 6 A M or something. I don't really care any longer as long as you will please conclude your investigation where I am concerned. My mistake, I believe, was in not getting my phone number changed back in the summer some time after I took down the BBS from my line. If these freaks or whatnot have passed my number around there is not one thing I can do about it.

You also noted that I had a post office box. Yes I do and have had for many years. It is actually registered for this building I think and not just for my use. You kept talking about Hyde Park New York, or Chicago. I was born in [redacted], raised in [redacted] This was supposed to be some other coincidence of yours. Believe me, no one who values their life lives in Hyde Park, a south side ghetto here. No I guess you dont believe anything I say . b6 b7C

You keep asking where I was teaching school. I am not a school teacher, I am not competent to teach much of anything, and I was not teaching anything last summer or any other time. You made a big thing of me having some kind of trouble with the phone company. I tried to explain to you that in November (two months ago!) I got billed for some extra units that was supposed to be on my call pack. I don't know how you keep relating this to some sort of phone trouble from last summer.

b6
b7C

Believe me, sir, I intend absolutely no disrespect for your office or your investigation, but there is nothing further I can tell you except to continue repeating myself as I have done.

If you persist that I must come to Virginia it will work a very bad hardship for me. I have little money, and none to spare for travel, etc. I will lose time (and money) from work. I am already indebted at work and just keeping afloat, due to a theivery here in June for which I was held accountable because of careless handling of the office money. (Sneak theif while my back was turned). I am just now finally getting that money, almost two thousand dollars paid off to the owner. I live from one two hundred dollar paycheck to the next. If I had to come over there, there is no way I could even buy the ticket right now.

May I offer what I hope will be satisfactory to you? I will submit to a lie detector test by anyone you choose. It could be your Chicago office. I will also answer any questions a grand jury might want to ask, and possibly this can be notorized or something in your Chicago office.

I am not trying to avoid you in anyway, but there is nothing further I can tell you about [redacted] or [redacted]. I am not these people and I do not know these people. I am tired of being harrassed by people looking for them, and I do not want more mail coming to [redacted]. Also I do not like the repeated insinuations about trouble for myself. I cannot even afford an attorney for advice regarding this letter but I am trying to write you in a frank and honest way. I want to clear myself immediatly and with no further delay. I do not know any of the other names you mentioned, except that the name [redacted] stood out, I remembered the fellow in Texas using that name. This whole matter has me very upset and frankly because of my financial situation at present I am thinking maybe I will sell the computer and forget about the BBS since its only a hobby for me anyway. I would not even have the money to buy a computer these days -- I did a couple years ago when I first got it.

b6
b7C

If there is ANYTHING further I can do, please let me know, but I sure want to clear myself if possible right here through your Chicago office for the reasons mentioned. I am sending this to you by registered mail to insure that you personally get it, and hope to have a reply from you shortly. I do appreciate your efforts but I have nothing to do with your problem. Permit me to clear myself if you are so suspicious of me. Thank you.

Sincerely yours,

[redacted]

[redacted]

b6
b7C

F47 76

PS --

I talked just a few minutes ago to [redacted].

b6
b7C

He says he told you about [redacted] being on the BBS run by [redacted] at the Library. (NOT EVER SEEN BY ME)

He says he also told of how those freaks almost wrecked my other BBS when I was running it with [redacted]. (Think BBS). (Was on other phone line) He mentioned several names to you of those people..

b6
b7C

[redacted]

all of whom are a bunch of young kids who like to destroy anything someone else starts.

Also he said you asked xx about "all my phone lines.."

I have 3 lines

[redacted]

b6
b7C

The first is for our office in the apartment building. The second is more for outgoing calls (it has a call pack) we use it both in the office and for me. Also used by xxxx janitor, etc.

The third used to be for me privately, now its the BBS I operate after the fools trashed my other thing.

If there is anything further at all let me know. Can I take a lie detector test?

[redacted]

b6
b7C

[redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS	
[redacted]	AHSC	$62.29	July, August, September	
	UAW	$31.00	September	
[redacted]	Maraven	$16.00	August, September	b6 b7C
	Telenet	$108.00	July, August	
[redacted]	BMW	$0.29	September	
		$127.58		
[redacted]	CBOT	$2.00	September	b6 b7C
[redacted]	RADA	$1.00	September	
		$3.00		
[redacted]	Maraven	$24.00	August	
	Telenet	$325.00	July	b6 b7C
	Telenet	$151.00	August	

SC13P [redacted]

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F49 40

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/15/83

The following is a summary of messages left by the illegal user known as [redacted] and [redacted] on GTE Telemail. b6 b7C

The date and time of each message is provided with a synopsis of particularly significant messages included.

1) August 30, 1983, 12:57 a.m.
2) August 30, 1983, 1:07 a.m.
3) August 30, 1983, 1:12 a.m.
4) August 30, 1983, 1:18 a.m. This message is from "Kaybis" to [redacted]. The message reads, "Through the airport?? You think a kilo would be a bit obvious. I know John Delorean, ya know." b6 b7C
5) August 30, 1983, 1:30 a.m. This message reads, "What happens when the dogs eat my leg??"
6) September 1, 1983, 5:12 p.m. This message reads, "Hello [redacted] and anyone else reading this text. [redacted] that hoochie is 100%! I've already gone through half what I bought. I'm gonna save the rest and buy another. Anyone interested in trading MCI nodes and codes?" b6 b7C
7) September 8, 1983, 10:27 p.m. This message reads in part, '[redacted], as of 7:30 this evening, I have not heard anything on our 'shipment'." b6 b7C
8) September 8, 1983, 10:30 p.m. This message reads, '[redacted], I let our computer phone number search program run for about three hours tonight. All I got was a shit load of Telenet accesses. Ah well call me huh?"
9) September 10, 1983, 11:21 p.m.
10) September 10, 1983, 11:24 p.m.
11) September 13, 1983, 12:53 a.m.
12) September 21, 1983, 12:07 a.m.

Investigation on 12/9/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :btl Date dictated 12/9/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F54 85

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/1/83

The following is a review of evidence seized pursuant to a Federally approved search warrant conducted at [redacted] on October 12, 1983. b6 b7C

The following is a summary of the evidence that is relevant to this investigation:

(1) A brown heavy paper envelope that was addressed to [redacted] (No last name written), [redacted] and the return address is [redacted], [redacted] is also known as [redacted] b6 b7C

(2) A packet of white sheets of paper stapled together. On the first sheet is the term [redacted] followed by the number [redacted] On the second page of this item is the name [redacted] and the address [redacted]. From this same sheet of paper is a number [redacted] and the numbers 1, 123, and the password [redacted] " This phone number is the modem phone number for [redacted] and the numbers and password are the account number and password for [redacted] on that bulletin board. b6 b7C

(3) This item is a scrap of greenish paper containing numerous telephone numbers. On that sheet of paper is the word "Mail" followed by a dash and the word "Phones" followed by another dash and the word "Phones" again. That sequence of words allows a person to get every Telenet dial up number from the Telemail System.

(4) A scrap of white paper with four telephone numbers on it. Also appearing on the sheet of paper is the name [redacted] b6 b7C

Investigation on 11/15/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :plw Date dictated 11/15/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(5) A sheet of white paper with the number [redacted] written on it. b6 b7C

(6) A computer print-out that came from [redacted] bulletin board. This message is from [redacted] and it is about the ITT Dialcom Network. In this message, [redacted] leaves an ITT Dialcom account and password. [redacted] also says he has about seven other accounts on ITT Dialcom. b6 b7C

(8) A computer print-out from [redacted] bulletin board from [redacted]. In this message he gives the telephone number for the University of Kentucky computer and gives you a log-in code. [redacted] also leaves five source accounts with the instructions to dial up Telenet and stating that you can access the source system by hitting "C" then a space then "30128" on your keyboard. This message is followed by another message from [redacted] in which he lists at least 75 main frame computers and their telephone numbers. Examples of the computers are Michigan National Bank, University of Hartford, Charge Card Association, Michigan Bell. b6 b7C

(9) A print-out of a "telephone modem search" by [redacted] with sub-routines by [redacted]. b6 b7C

(10) A photocopy entitled, "Local Telephone Numbers for Access to the SPRINT Network."

(11) A computer print-out entitled, "How to Cause Car Trouble." This lists numerous things a person can do to damage an automobile such as "Pour Draino in the radiator. Pour sand in the crank case," and numerous other methods for damaging someone's car.

~~F56~~

47

FD-302 (Rev. 3-10-82)

Extra Copy
Do Keep

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/16/84

[redacted], a computer programmer, examined various "floppy disks" that were seized pursuant to a Federally approved search warrant at the residence known as [redacted]. This is the residence of [redacted], and his parents. b6 b7C

[redacted] found the following information of interest: b6 b7C

On a floppy disk labelled 196-633-Sub I 1B1, Item Number 3 (one of eight), Number 1, the following information was found: Under a heading "OMNICOD/BAS" appears a program that searches for access codes to computers or long distance networks. Under a heading known as "SPCODE/BAS" appears a program that will break MCI "access codes" or other similar services. A program labelled "SPTRVCD/BAS" appears to also attempt to break long distance access codes. A program known as "COMFIND" searches for other computers via the phone.

On the floppy disk labelled 196-633-Sub I, 1B1, Item Number 3 (two of eight), Number 4, [redacted] found the following programs: "Code Breaker for the Hayes Smartmodem". This program tries different access codes for a given phone nubmer, probably to get access codes for a long distance service like MCI. b6 b7C

A program known as "Breaker/BAS" is a program similar to the one above, but slightly more sophisticated.

A program known as "Break/BAS" appears to be an earlier version of "Breaker/BAS".

On the disk labelled 196-633-Sub I, 1B1, Item Number 3 (one of eight), Number 3, [redacted] found the following: A program labelled "Message/TXT". This is a listing of various messages left on a home bulletin board set up by [redacted]. The program known as "Member/DAT" is a listing of various people authorized to use [redacted] "bulletin board". b6 b7C

Investigation on 1/10/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted]:gaj Date dictated 1/11/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F57 88

On the disk known as 196-633-Sub I, 1B1, Item Number 3 (one of eight), Number 2, [redacted] found a program labelled "PHONE/TXT". This is a listing of messages from the Osuny bulletin board. b6 b7C

On the disk labelled 196-633-Sub I, 1B1, Item Number 1, Number 4, [redacted] found a program labelled "COMPROG/BAS". This is the beginning of a program to search for other computers over the phone. On the program labelled "CODE" appears a program to find codes for services like MCI. [redacted] also found three programs labelled "COMV3/BAS", "COMFIND/BAS", and "COMMFID/BAS", all of which are programs to search for other computers by the phone. The program labelled "TRAVCOD" is the same program as the previous one labelled "CODE". b6 b7C

On the floppy disk labelled 196-633-Sub I, 1B1, Item Number 1, Number 6, [redacted] found the following programs: A program labelled "COMV41" which is a program for searching for computers by phone. A program labelled "FINDINGS" lists the results of the program produced by "COMV41". A program labelled "MCIV41" searches for MCI access codes. A program labelled "MCIFIND" lists the results of the above program. b6 b7C

On the floppy disk labelled 196-633-Sub I, 1B1, Item Number 1, Number 8, [redacted] found the program "RUSERS/LOG". This program lists various users from a home bulletin board. b6 b7C

On the disk labelled 196-633-Sub I, 1B1, Item Number 1, Number 13, [redacted] found a program labelled "FINDINGS". This program lists the results of a computer search program, apparently from the previous program labelled "COMV41". b6 b7C

~~F58~~

89

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS	
[redacted]	AHSC	$62.29	July, August, September	
	UAW	$31.00	September	
[redacted]	Maraven	$16.00	August, September	b6 b7C
	Telenet	$108.00	July, August	
[redacted]	BMW	$0.29	September	
		$127.58		
[redacted]	CBOT	$2.00	September	b6 b7C
[redacted]	RADA	$1.00	September	
		$3.00		
[redacted]	Maraven	$24.00	August	b6 b7C
	Telenet	$325.00	July	
	Telenet	$151.00	August	

Sub I

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F59 90

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/5/84

The following is a summary of messages left by the illegal user known as [redacted] on the GTE Telemail system. The date and time of each message is provided, with a synopsis of particularly significant messages included. b6 b7C

1.) July 7, 1983, 8:49 PM (all times eastern daylight time).

2.) August 17, 1983, 12:26 AM.

3.) August 17, 1983, 2:50 PM. This message reads, "Are you serious [redacted]? What's this younger generation coming to." b6 b7C

4.) August 17, 1983, 5:20 PM.

5.) August 18, 1983, 5:48 PM.

6.) August 15, 1983, 7:16 PM.

7.) August 17, 1983, 7:35 PM.

8.) August 18, 1983, 7:54 PM.

9.) August 20, 1983, 8:31 PM. This message reads, "Did you know that 202141 is the same as Telemail? I didn't."

10.) August 24, 1983, 6:52 AM.

11.) August 27, 1983, 12:44 AM. This message is to [redacted] and is signed [redacted]. b6 b7C

12.) August 27, 1983, 4:45 AM. The content of this message indicates that [redacted] first name is [redacted] and that he knows the home phone number to the hacker known as [redacted]. This message also indicates that this person talked to the manager of a computer system and threatened to damage their computer system. b6 b7C

Investigation on 12/8/83 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted]:gaj Date dictated 12/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F64 95

13.) August 27, 1983, 6:13 AM.

14.) August 27, 1983, 2:46 PM.

15.) August 29, 1983, 4:03 PM. This message is from Admin/Raytheon to [redacted]. The message reads as follows: "This is [redacted]. You may want to change the PWD until [redacted] cools off. I didn't REG my user name, but I'd like one. Signed [redacted]." b6 b7C

16.) August 29, 1983, 8:04 PM.

17.) August 29, 1983, 10:03 PM.

18.) August 31, 1983, 1:51 PM.

19.) September 1, 1983, 4:13 AM.

20.) September 3, 1983, 2:34 AM.

21.) September 4, 1983, 4:46 PM.

22.) September 4, 1983, 4:59 PM.

23.) September 6, 1983, 3:51 PM.

24.) September 7, 1983, 2:45 AM.

25.) September 6, 1983, 7:31 PM.

26.) September 6, 1983, 3:54 PM.

27.) September 10, 1983, 1:30 AM.

28.) September 10, 1983, 2:31 PM.

29.) September 11, 1983, 4:00 AM. This message reads, "[redacted] is [redacted] (not the original) who runs [redacted] is a phreak. Nothing special." [redacted] is the home bulletin board run by [redacted] (aka [redacted]) who was a subject in this matter. b6 b7C

30.) September 13, 1983, 2:51 PM. This message reads in part, "There's no telling how long this will be up, but I have been on here for about a year with no problems."

~~E65~~

31.) September 13, 1983, 11:21 PM. This message reads as follows: "The people at Telenet will know we're here sooner or later and they may or may not get angry; so don't post things that give your name or number and you may want to use a node other than your own. Some phreaks loop their calls all over the U.S."

32.) September 14, 1983, 3:25 AM. This message reads in part, "We are not the only phreak people on the system, and [redacted] got the FBI after him by deleting Nasa's major node." The message also contains the sentence, "I was also a member of both PHA and Innercircle and am now a member of Securityland." This message also contains the PS: "All this talk about who I am (sic) because I can see how great this would be if I worked for the FBI." b6 b7C

33.) September 14, 1983, 10:37 PM. This message is from [redacted] to [redacted] and reads, "Hi [redacted].Well I also have been hacking on Telenet for quite a while (not as long as you) and this is not my only T-mail admin. This group is not really mine but I adopted them because I plan on dumping Telemail soon anyway (very strong rumors that Nasa had some major trouble and had the FBI on Telemail). For this reason I won't give away anything else, except that if you can get on [redacted] board you can contact me there. Quite a project if you're government. I'd also like to say that I left everything open here on purpose figuring that if Telenet was looking for me they would find me otherwise I don't care who sees this. We do have more private groups though. Signed [redacted]." b6 b7C

34.) September 14, 1983, 10:42 PM. This message is from Admin/SCPP/Bang/Promo/Raytheon to SCPP. Subject is: [redacted]. Text of the message is "I am [redacted] and my address is [redacted]." b6 b7C

35.) September 15, 1983, 1:29 AM. This is from Admin/Promo/Raytheon to SCPP, subject "Also [redacted]. Text of the message is "I am also The [redacted].Only in a more powerful state." b6 b7C

36.) September 15, 1983, 1:27 AM.

37.) September 15, 1983, 1:15 AM. This message reads as follows: "The Telenet people can easily find out which node you call from; in fact, it will be on the bill to be sent out about now. But many Admins don't look for the user name or anything like that. Oh yes, I do not work for the FBI."

38.) September 15, 1983, 1:59 AM.

39.) September 15, 1983, 2:00 AM.

40.) September 15, 1983, 1:19 AM.

41.) September 15, 1983, 1:32 AM.

42.) September 15, 1983, 4:18 PM. The text of this message is as follows: "Oh it was just a thought...I had heard that the FBI was looking into Telmail (SIC) because someone deleted Nasa and Unix...True? I know someone who told me they deleted Unix a while back and he could well have deleted Nassa. Signed [redacted]." b6 b7C

43.) September 15, 1983, 7:49 PM.

44.) September 16, 1983, 4:30 AM.

45.) September 16, 1983, 5:42 PM.

46.) September 17, 1983, 3:24 AM.

47.) September 18, 1983, 4:01 AM.

48.) September 19, 1983, 6:21 AM.

49.) September 21, 1983, 5:55 AM.

50.) September 23, 1983, 4:24 AM.

51.) September 24, 1983, 6:35 AM. This message reads in part, "Ah you shouldn't have mentioned the Oak Industries Vax, now you'll have to hear how I broke in on their Vax and had them beg for mercy."

The message continues, "Well it's been almost two years and I just got a breakthrough that will give me an account before too long. I don't know whether to use it for years quietly or destroy the Vax."

52.) September 24, 1983, 6:20 PM.

53.) September 26, 1983, 2:31 AM.

54.) September 27, 1983, 2:32 AM.

55.) September 27, 1983, 5:55 AM.

56.) September 27, 1983, 5:56 AM.

57.) September 27, 1983, 6:10 AM. This message reads in part, "When I was a member of PHA (Phreakers of America) and two generations of TIC (The Innercircle) we did all kinds of things that did nothing but waste time, to show that we were a group. We set up and took down boards, argued over different logos, voted members we didn't like out, etc."

58.) September 29, 1983, 7:12 PM.

59.) October 1, 1983, 9:17 PM.

60.) October 2, 1983, 4:30 PM.

61.) October 2, 1983, 4:33 PM.

62.) October 3, 1983, 7:55 PM.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 12/28/83

The following is a review of items seized in a court authorized search of the premises known as [redacted], on October 13, 1983. The following items of relevance to this investigation were found: b6 b7C

1) A spiral bound notebook containing the name [redacted] and the telephone number [redacted]. b6 b7C

2) A letter from [redacted]. This letter discusses some sort of a computer war game that both [redacted] and [redacted] are involved in. b6 b7C

3) A post card from [redacted]. This post card appears to discuss a computer war game that [redacted] and [redacted] are involved in. b6 b7C

4) A white 3-inch by 5-inch card bearing the name [redacted], telephone number [redacted], address [redacted] b6 b7C

5) A white 3-inch by 5-inch card bearing the name [redacted], telephone number [redacted], address [redacted] b6 b7C

6) A white 3-inch by 5-inch card bearing the name [redacted], telephone number [redacted], address [redacted] b6 b7C

7) A 9-inch by 12-inch water color pad with the first page bearing the following information: [redacted]. This sheet of paper also bears the telephone number [redacted] followed by the word [redacted]. It also has the telephone number [redacted] followed by the name [redacted]. It also contains the telephone number [redacted]. The note pad also bears the name [redacted] followed by the telephone number [redacted]. This pad also has the name [redacted] followed by the telephone number [redacted]. b6 b7C

Investigation on 12/22/83 at Alexandria, Virginia File # Alexandria 196A-633 Sub F

by SA [redacted]:btd Date dictated 12/22/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F69 100

8) A white sheet of paper bearing the telephone number [redacted]. b6 b7C

9) A white card bearing numerous telephone numbers and a dial up number and access code for Ditt DialCom Computer System.

10) Approximately 30 sheets of computer paper stapled together and labeled RDF Start Up Routines.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS	
[redacted]	AHSC	$62.29	July, August, September	
	UAW	$31.00	September	
[redacted]	Maraven	$16.00	August, September	b6 b7C
	Telenet	$108.00	July, August	
[redacted]	BMW	$0.29	September	
		$127.58		
[redacted]	CBOT	$2.00	September	b6 b7C
[redacted]	RADA	$1.00	September	
		$3.00		
[redacted]	Maraven	$24.00	August	b6 b7C
	Telenet	$325.00	July	
	Telenet	$151.00	August	

SUB F

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~FBI~~ 102

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 1/4/84

The following is a summary of messages left by the illegal user using the names [redacted] and [redacted] on GTE Telemail. b6 b7C

The day and time of each message is provided, with a synopsis of particularly significant messages indicated.

1. July 10, 1983, 5:33 p.m.
2. July 16, 1983, 12:32 a.m.
3. August 2, 1983, 7:06 p.m.
4. August 5, 1983, 2:46 a.m.
5. August 8, 1983, 10:08 p.m.
6. August 10, 1983, 10:01 a.m.
7. August 10, 1983, 11:00 a.m.
8. August 10, 1983, 10:46 p.m.
9. August 12, 1983, 6:39 p.m.
10. August 26, 1983, 12:40 a.m.
11. August 26, 1983, 12:46 a.m.
12. August 28, 1983, 12:54 a.m.
13. August 28, 1983, 1:02 a.m.
14. August 31, 1983, 9:32 p.m.
15. September 3, 1983, 10:49 p.m.
16. September 4, 1983, 7:02 p.m.
17. September 10, 1983, 7:18 p.m.
18. September 10, 1983, 7:31 p.m.
19. September 12, 1983, 11:16 p.m.
20. September 12, 1983, 11:08 p.m.
21. September 12, 1983, 11:17 p.m.
22. September 12, 1983, 11:37 p.m.
23. September 15, 1983, 11:05 p.m.
24. September 15, 1983, 11:09 p.m.
25. September 15, 1983, 11:12 p.m.

This message reads "Does anyone think we will be better off if we made a separate phone call for each connection to telemail? Would that make us look more like the real thing?"

Investigation on 12/8/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :gkh Date dictated 12/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F76 107

September 16, 1983, 8:17 p.m.
September 18, 1983, 2:09 a.m.
September 19, 1983, 12:24 a.m.
September 19, 1983, 11:44 p.m.
September 22, 1983, 10:45 p.m.
September 26, 1983, 9:12 p.m.
September 28, 1983, 7:44 p.m.
September 28, 1983, 7:45 p.m.
September 28, 1983, 8:39 p.m.
September 29, 1983, 11:28 p.m.
September 29, 1983, 11:48 p.m.
October 1, 1983, 7:35 p.m.
October 2, 1983, 9:51 a.m.
October 2, 1983, 11:35 p.m.
October 9, 1983, 12:21 a.m.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/5/83

The following is a summary of the review of seized evidence obtained pursuant to a duly-authorized Federal search warrant executed on October 12, 1983, at the residence of [redacted]. b6 b7C

The following is a summary of the evidence that is relevant to this investigation:

1. A computer card bearing the number 800-424-9494, with the word "telenet" written underneath it;

2. A computer card with the words [redacted] and [redacted] written on it; also written on this card are the words "cbot", "scannet", "dialcom", and "tymnet"; this card also contains the word [redacted]; b6 b7C

3. This item is a yellow sheet of paper with numerous phone numbers associated with bulletin boards; also found on this sheet of paper is the number [redacted], followed by the word "Voice" and the name [redacted]; this sheet of paper also bears the address [redacted]; it also contains the name [redacted], followed by the telephone number [redacted]; b6 b7C

4. A white sheet of paper bearing numerous phone numbers, some of them identified as follows: [redacted]. This paper also contains the name [redacted], and the number [redacted], and the name [redacted] and the number [redacted]; b6 b7C

5. A message addressed to [redacted], dated 6:00 PM, September 15, 1983. It is addressed to [redacted] and in the remarks section it says, "[redacted] called. Be on campus 9:00 [redacted], Number [redacted]." On the back of this message are the words [redacted] and [redacted]; b6 b7C

Investigation on 11/15/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:sfk Date dictated 11/15/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F78 109

6. White sheet of paper with the name [redacted] - [redacted]. It also contains the name [redacted] and next to that the word [redacted]. This sheet of paper also contains the name [redacted] and [redacted]; b6 b7C

7. A white sheet of computer paper with the word "Black" and the number "800-523-0684". This sheet of paper also bears the word "NASA", "ARC", "JPL". These are all host companies on telemail that were penetrated by hackers;

8. A white sheet of paper bearing "[redacted] = [redacted]; [redacted] = [redacted] = [redacted] = [redacted]". This sheet of paper also has the words telemail check; b6 b7C

9. A white sheet of computer print-out paper that has numbers listed for ITT, Metrofone, Telenet, Sourcenet, Sprint, followed by what appeared to Sprint access codes; Allnet and two 800 numbers;

10. A sheet of computer print-out paper that has the word Maraven, followed by the words [redacted], [redacted] and [redacted]; followed by the word phalse. This sheet of paper also has the words [redacted], and [redacted]. b6 b7C

~~P79~~

110

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS
[redacted]	AHSC	$62.29	July, August, September
	UAW	$31.00	September
[redacted]	Maraven	$16.00	August, September
	Telenet	$108.00	July, August
[redacted]	BMW	$0.29	September
		$127.58	
[redacted]	CBOT	$2.00	September
[redacted]	RADA	$1.00	September
		$3.00	
[redacted]	Maraven	$24.00	August
	Telenet	$325.00	July
	Telenet	$151.00	August

b6 b7C

b6 b7C

b6 b7C

b6 b7C

5033 [redacted]

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~FBI~~ 112

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 1/4/84

The following is a summary of messages left by the illegal user using the name [redacted] on GTE Telemail. The date and time of each message is provided, with a synopsis of particularly significant messages included. b6 b7C

1.) August 15, 1983, 12:17 AM.

2.) August 15, 1983, 12:24 AM.

3.) August 18, 1983, 1:18 AM.

4.) August 19, 1983, 12:18 AM.

Investigation on 12/8/83 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 12/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F86 117

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS
[redacted]	AHSC	$62.29	July, August, September
	UAW	$31.00	September
[redacted]	Maraven	$16.00	August, September
	Telenet	$108.00	July, August
[redacted]	BMW	$0.29	September
		$127.58	
[redacted]	CBOT	$2.00	September
[redacted]	RADA	$1.00	September
		$3.00	
[redacted]	Maraven	$24.00	August
	Telenet	$325.00	July
	Telenet	$151.00	August

b6 b7C

SAB [redacted]

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~F88~~ 119

AX 196A-633

IDENTIFICATION RECORDS, PRIOR ARRESTS,
SCIENTIFIC AND TECHNICAL REPORTS:

AX 196A-633

TABLE OF CONTENTS

FOR REPORT FORMS (FD-302's)

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 2/15/84

The following is a summary of the activities of [redacted], aka [redacted], on GTE Telemail. b6 b7C

[redacted], using the alias [redacted], was an illegal user in three different telemail companies as follows:

AMERICAN HOSPITAL SUPPLY COMPANY (AHSC)
RADA COMPANY
MMM COMPANY

[redacted] is known to have left at least ten messages on the GTE Telemail System from August 31, 1983, to October 11, 1983. b6 b7C

In late September, 1983, [redacted] began "welcoming" new illegal users to the telemail system.

On September 20, 1983, September 21, 1983, September 22, 1983, September 23, 1983, and again on September 24, 1983, the GTE Telemail security log detected a hacker attempting to break into forty different legitimate telemail administrator accounts. All of these calls came from the 402 area code and into telenet dial-in number [redacted]. Trap and trace records received from [redacted] b6 b7C b7E

Investigation on 2/2/84 at Alexandria, Virginia File # Alexandria 196A-633 Sub T

by SA [redacted]:tro Date dictated 2/2/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

5

128

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 10/18/83

On October 13, 1983, a male identifying himself as [redacted] telephonically contacted the Omaha office of the Federal Bureau of Investigation (FBI) and stated that he was at that time in San Diego, California. [redacted] continued that he had been informed that his [redacted] residence had been "ransacked," and that "some piece of paper" had been left at his house. b6 b7C

[redacted] was informed that his home had been searched on October 12, 1983, by Special Agents (SAs) of the FBI, pursuant to a warrant issued by a U. S. Magistrate for the Southern District of Iowa (SDI), and that since no one could be found at the residence, a copy of the warrant and inventory of all items seized by authority of the warrant was prominently attached to the front of the regrigerator in the kitchen of his residence. b6 b7C

[redacted] was further informed that his use of the word "ransacked" was inaccurate in that upon entry to the residence, SAs noted that every room in the residence was in a state of total disarray. b6 b7C

[redacted] stated he was concerned that his professional papers had been seized and he could not conduct his business without them. b6 b7C

He was informed that items taken were selectively seized as being related to or evidence of the criminal conduct specified in the search warrant, Fraud By Wire (FBW).

[redacted] stated he had been at his home on only four occasions during the last two months, and wondered whether some "kids" may have been using his computer. b6 b7C

[redacted] added that his house is always open, and anyone can enter the house at any time. b6 b7C

Investigation on 10/13/83 at Omaha, Nebraska File # Omaha 196A-922

by SSA [redacted] :cac Date dictated 10/13/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 2/2/84

The following is a summary of the activities of [redacted], on telemail.

b6
b7C

[redacted] used the names [redacted] and [redacted] in the companies known as RADA and MMM. [redacted] has accessed telemail approximately 12 times from August 30, 1983, to September 21, 1983.

His messages include references to drug usage and plans for interstate transportation of drugs and to "trading" MCI long distance access codes.

On October 12, 1983, [redacted] admitted to accessing GTE telemail to communicate with [redacted] and [redacted].

b6
b7C

Investigation on 1/30/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:mbe Date dictated 1/30/84

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

X 130

FD-302 (REV. 3-8-77)

FX 196A-1325

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 10/17/83

At 6 A.M., on October 12, 1983, [redacted], were awakened at their residence at [redacted] at which time they were advised as to the identities of the interviewing Agents and the purpose for the Agents being at their residence. b6 b7C

At 6 A.M., a search warrant was served on [redacted] for the search of his residence, [redacted] advised his son did have a computer and it was located in his son's room. At this time [redacted], was awakened and advised as to the identities of the Agents and the purpose for their presence. At this time [redacted], appeared to be hyperventilating. [redacted], explained to the Agents where his records were concerning his computer. [redacted], pointed out the one diskett that contained all the computer records of his use of General Telephone and Electronics' (GTE) Telemail. SA [redacted] wrote "Telemail" on the corner of this disk. [redacted], was then taken to the kitchen and interviewed in the presence of his father. b6 b7C

Both [redacted] and [redacted], were advised that [redacted], was a subject in the investigation, however, there was no arrest warrant for his arrest and further that he was not going to be arrested on this date. [redacted] was advised that he did not have to talk to the FBI, however, he was asked if he did wish to be interviewed to which he stated he was willing to talk to the FBI. At this time [redacted], provided the following information: b6 b7C

Approximately two to three months past he was using his computer through Compuserve, a service he was paying for out of Columbus, Ohio. His access number in Tucson, Arizona, for Compuserve is [redacted]. This is an open line that can be used like a CB radio. Anyone can talk to anyone that subscribes to this service. Through Compuserve he talked to an individual who used the name [redacted]. He does not know if [redacted] was a true name or not. [redacted] told him he could use GTE's Telenet system to send messages. [redacted] told him to dial Telenet, 747-0107 and then type in Telemail. First account [redacted] gave him was [redacted]. Later he told him his [redacted] account was [redacted]. b6 b7C

He did send messages and talk to people using the GTE Telenet System. He talked with [redacted] (true name not recalled) (SUBJ)

FX 196A-1325-5

Investigation on 10/12/83 at [redacted] File # Phoenix 196A-1325

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]

by SAs [redacted] and [redacted]:ERH:/jar Date dictated 10/14/83 b6 b7C

OCT 31 1983

FBI — ALEXANDRIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

8 131

who is a male who said he lived close to Los Angeles, California. He located a note from his records that reflected [redacted] telephone number as [redacted]. He also located a brown envelope from his records that he had received from [redacted] which reflected a return address of [redacted] b6 b7C

[redacted] true name is [redacted] whose residence telephone number is [redacted] and bulletin board number is [redacted]. b6 b7C

[redacted] true name is [redacted]. He located a note from his record reflecting the name [redacted] and address [redacted]. He advised that [redacted] telephone number is [redacted]. b6 b7C

He talked to [redacted] and [redacted] over the Telemail accounts. b6 b7C

He remembers seeing the name [redacted] on Telemail and believes [redacted] lives in [redacted] used the codename [redacted]. He saw one message in which the name [redacted] was used instead of codename [redacted] in which [redacted] said he was going to Detroit for a CB conference. [redacted] was always bragging about changing the pass words in the computer of Miter Corporation, Arpanet System, which is designed for research corporations. He changed the pass words because the systems administrative caught him in the system and told him to get off. In talking with [redacted] on Compuserve he asked [redacted] what happened to his account, [redacted], in that he tried to use it and it was not there. [redacted] told him some of the accounts had been erased and that [redacted] was trying to set up new accounts. b6 b7C

[redacted], true name unknown, told [redacted] how to access Telemail. In a conference call between [redacted] and himself, [redacted] was bragging about his use of the Arpanet System. [redacted] also bragged and said that he had erased 200 NASA Accounts. [redacted] had more knowledge about the Telemail system than anyone else. b6 b7C

[redacted] was a Hacker who used both Compuserve and Telemail who he believes lives in Oklahoma City. He does not know the true name for [redacted]. He sent and received messages from [redacted] and through these messages [redacted] said he lived in [redacted] and [redacted] did not live far away. In conversations with [redacted] said he lived within an hour of [redacted]. b6 b7C

He talked with [redacted] on Compuserve and saw [redacted] name on Telemail. He did not use Telemail to talk with [redacted]. He believes [redacted] is a friend of [redacted] and [redacted] and that [redacted] said he [redacted] had gone to a party with [redacted] and [redacted]. He believes several people used the codename of [redacted]. b6 b7C

He recalls seeing the name [redacted] (codename) on Telemail and believes he may live in New York. b6 b7C

[redacted] told him he [redacted] had gotten his new account for Telemail from [redacted] over Compuserve. b6 b7C

[redacted] gave him his new account, name of [redacted]. He does not know where [redacted] got the new account. However in later conversations with [redacted] and [redacted] he was told by them that [redacted] had set up the new account. b6 b7C

He believes [redacted] was the one who started illegally using Telemail. b6 b7C

[redacted] gave him an account number 405,206 and the password "Bad Boy" to enter the University of Kentucky Dec Systems 10. [redacted] of Dec Systems 10 is [redacted], telephone number [redacted]. He was on the system when [redacted] gave him [redacted] the account number and password. [redacted] said it was okay to use the system as long as they did not erase any files. b6 b7C

[redacted] also used SOURCE which is a GTE Telenet System and is similar to Compuserve. [redacted] erased a lot of one section of the computer in SOURCE. They were aware that [redacted] erased the system but they did not know who [redacted] was. They closed all the accounts under the name [redacted]. b6 b7C

The codename [redacted] was also used in conjunction with the codename [redacted] and that he believes [redacted] true name is [redacted] (Last Name Unknown) who either lives in [redacted]. b6 b7C

[redacted] (codename) true name unknown, lives in [redacted] and also uses [redacted] bulletin board, telephone number [redacted]. [redacted] was telling everybody how to access Sprint and other telephone systems. b6 b7C

[redacted] also told people how to make boxes that produced tones to access telephone systems without paying. [redacted] offered these boxes for sale for $30 each. [redacted] said he was [redacted] years old and his telephone number is [redacted]. b6 b7C

He also advised that [redacted] also sent him information on how to access Sprint. b6 b7C

He did not know any of these individuals prior to the use of Telemail nor has he ever personally met them. He did not know any of these systems were being illegally used and he did not profit in any way from the use of Telemail.

[redacted], is described as follows:

Race:	[redacted]	b6 b7C
Sex:		
Date of Birth:		
Height:		
Weight:		
Hair:		
Eyes:		
Social Security Account Number:	[redacted]	
Residence:	[redacted]	
Arizona Driver's License Number:	[redacted]	b6 b7C
Father:	[redacted]	
Employed:	[redacted]	

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 2/2/84

This is a summary of the activity of [redacted] on GTE telemail: b6 b7C

[redacted] used the names, [redacted], and [redacted] on telemail. b6 b7C

[redacted], using the name [redacted], was a member of the "Inner Circle," and illegal group in the company AHSC, and was also an illegal user in a company called Raytheon, as ADMIN/SCPP/BANG/PROMO/RAYTHEON.

[redacted] is known to have accessed the telemail system, using one of the above aliases, approximately 62 times, from July 7, 1983 to October 3, 1983. b6 b7C

GTE logs show that [redacted] would access the telemail system through the dial-up and the 619 area code. b6 b7C

On October 12, 1983, [redacted], aka, [redacted], stated to FBI agents that [redacted] was [redacted] telephone number [redacted]. A search of [redacted] residence also produced an envelope with the above return address. b6 b7C

On October 14, 1983, [redacted] stated to the FBI that he was [redacted] on telemail and provided additional details of his telemail intrusions. b6 b7C

Investigation on 1/30/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:mbe Date dictated 1/30/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/1/83

On October 13, 1983, [redacted] was interviewed at her place of residence, [redacted], while that residence was being searched by Special Agents (SAs) of the San Diego Federal Bureau of Investigation (FBI) Office pursuant to a search warrant signed by U.S. Magistrate J. Edward Harris. [redacted] was advised of the identity of the interviewing agent, the nature of the search and the interview, and she voluntarily furnished the following information: b6 b7C

[redacted] advised that she has been employed at the residence since March 21, 1983. She further advised that she lives at the residence and that her job is to clean the home and take care of the seven infants. [redacted] stated that she has seen a computer in one of the downstairs rooms, however, she has no knowledge as to who operates the computer or what is done with it. She further stated that she has never seen anyone operating the computer and that, "I only take care of the kids and keep the house clean." b6 b7C

The interview with [redacted] was conducted in Spanish. b6 b7C

Investigation on 10/13/83 at [redacted] File # SD 196B-1018-23

by SA [redacted] /jaf Date dictated 10/14/83 b6 b7C

SEARCHED [redacted] INDEXED [redacted] SERIALIZED [redacted] FILED [redacted]

DEC 14 1983

FBI — ALEXANDRIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

136

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/1/83

On October 13, 1983, a search was conducted at [redacted], in response to a search warrant signed by U.S. Magistrate J. Edward Harris. A report regarding that search has been made. b6 b7C

Shortly after the searching agents arrived at the location, a [redacted]-year old white male named [redacted], who identified himself as the brother of [redacted], was interviewed. [redacted] was at the residence at the time the search warrant was executed. [redacted] assisted in identifying other individuals in the residence at the time. They included: b6 b7C

[redacted], age [redacted]

[redacted], age [redacted] b6 b7C

[redacted], age [redacted]

[redacted] years old, and a neighbor

[redacted] stated that other children in the family were [redacted] all in school at the present time. b6 b7C

[redacted] said that his parents were [redacted]. They were both at work at their company, [redacted], phone [redacted], which is located in the Mira Mesa area of North San Diego. [redacted] stated that his father's name was formerly [redacted] but had changed it to [redacted] for reasons not known to the boy. He said that his brother, [redacted] did not like the new name and maintained the old one. He said that all of his brother's computer equipment was located in his bedroom so far as he knew. He indicated that so far as he knew, his brother had his computer hooked up to telephone number [redacted]. In addition, two other numbers came into his home, [redacted] and [redacted] b6 b7C

[redacted] was asked to identify his brother's computer friends, and the only person whom he could identify was a boy named [redacted] who currently works part-time at Poway High School. He was aware that his brother "talks" to other friends around the country about computer games and specifically mentioned the State of Alabama. b6 b7C

Investigation on 10/13/83 at [redacted] AX 196A-633 SD 196B-1018 -3C SD 87B-10472

by SA [redacted] /jaf Date dictated 10/13/83 b6 b7C

INDEXED SERIALIZED FILED FBI 1983 FBI — ALEXANDRIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7C

[redacted] essentially stayed with SA [redacted] throughout the search of the residence except for [redacted] room in the basement and other basement area rooms.

A sketch was made of the house and that sketch is maintained by the Federal Bureau of Investigation.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/3/83

At [redacted], Special Agents (SAs) [redacted] and [redacted] identified themselves to [redacted], and SA [redacted] explained to [redacted] that Federal Bureau of Investigation (FBI) agents were going to search that residence, and he was exhibited a copy of the search warrant. SA [redacted] explained to him that the items to be searched for included a computer and related equipment. He explained that those items were in his bedroom and he directed agents to that location. b6 b7C

Following that, SAs [redacted] and [redacted] arrived at the residence and commenced searching. b6 b7C

[redacted] was advised that he was free to remain in the bedroom if he wished, but his movements were not restricted and he could leave if he so desired.

SA [redacted] advised him that he was suspected of participating in the unauthorized computer services of the Telemail Company through "hacking". [redacted] stated he was willing to be interviewed and he furnished the following information: b6 b7C

His true given name is [redacted] and he was born on [redacted]. While [redacted] was still a juvenile, his father changed his (the father's) name to [redacted] did not know whether that meant his name was officially changed or not, but the name he uses is still [redacted] b6 b7C

His parents own a business known as [redacted], which sells [redacted]. b6 b7C

He stated he does know of people who gain access to computer systems without authorization, but he does not do so and does not even have the equipment to do so. He stated he has no modem, but he stated that he has had access to one which belongs to [redacted], who lives in [redacted], telephone [redacted], and attends computer classes at UCSD. [redacted] last used his modem about two and one-half weeks ago. [redacted] has used his modem and has used b6 b7C

Investigation on 10/13/83 at [redacted] SD 87D-10472 SD 196B-1018-39

by SA [redacted] SA NIW/jaf Date dictated 10/13/83 b6 b7C

FILED — INDEXED — SERIALIZED — DEC 1 1983 — FBI — ALEXANDRIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

16 139

his computer. He does not think that [redacted] would be involved in any illegal computer activities such as "hacking".

SA [redacted] asked him if he has ever heard of a person who uses the name [redacted] He stated he has heard of this person but not lately. He does not think this person is from this area. b6 b7C

[redacted] was asked about the name [redacted] and again he stated he has heard of this person but has never seen anything "posted" by him. He has heard that [redacted] and [redacted] "pirate" discs, meaning they copy discs. b6 b7C

He has not heard of search warrants in connection with hackers being served throughout the country within the last few days. He did hear there was an article in Time Magazine that there was some sort of legal action being taken against Our Planet, which is a network of computers, which he stated he has used in the past.

SA [redacted] asked him if he heard of Telemail, and he stated he has but is not sure where. He denied ever having to access that computer system. b6 b7C

SA [redacted] asked him again where he had heard of [redacted] and he stated he heard that name on the "Bulletin Boards", which is a computer system that is used to post messages. He denied ever having used that name. b6 b7C

SA [redacted] joined the interview and asked [redacted] who is high school math teacher was, and he stated it was [redacted] and he had one by the name of [redacted] and another one by the name of [redacted]. He stated he has no black friends who are interested in computers. b6 b7C

SA [redacted] asked him if he is interested in contests or if he has any family in Texas, and he stated he does not enter contests and has no family in Texas. b6 b7C

At this point SA [redacted] departed from the bedroom where the interview was being conducted and returned a few minutes later and the interview continued. b6 b7C

[redacted] was asked several questions regarding his relationship to an individual by the name [redacted] stated that the name [redacted] was recalled by him as someone with whom he had attended [redacted], but his b6 b7C

recollection of [redacted] was not clear. Other questions were posed of [redacted] regarding his relationship to [redacted] but those questions did not specifically pertain to the search nor the unauthorized use of Telemail Services. The results of the questioning regarding [redacted] have been set forth in another report and are available at the FBI in San Diego if necessary. b6 b7C

During the search of the residence at [redacted] SA [redacted] observed a phone located in a small office-type space located off of the kitchen area in the residence. The telephone had five buttons and two lines were active, numbers [redacted] and [redacted]. These numbers appeared at the buttons on the phone. In addition, two other numbers appeared as buttons on the telephone but appeared to be inactive. The numbers were [redacted] and [redacted]. b6 b7C

Located in that office-type room was a game printout dated January 17, 1983, showing an account number 7781. [redacted] advised that that printout involved a game sponsored by Flying Buffalo, Inc., Box 1467, Scottsdale, Arizona. The game printout pamphlet was seized. b6 b7C

In addition, SA [redacted] assisted in the search of [redacted] room as well as in the search of the remaining part of the house. b6 b7C

A copy of the search warrant and an inventory of the items seized was provided to [redacted] by SA [redacted]. The inventory of items seized is available at the FBI in San Diego, where the seized items were taken. b6 b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/18/83

[redacted] was interviewed at his residence, [redacted]. He was advised as to the identity of the interviewing agent and that the interview would concern his knowledge and participation in activities, now commonly known as "hacking," into General Telephone Electronics (GTE) Telemail System. He was advised of his rights and executed a waiver. He furnished the following information. b6 b7C

He has been "hacking" for approximately nine to ten months. He has always been interested in electronics and has built many electronic kits. Since he was very young, he has had interest in seeing how things were constructed. It is only of recent that he has developed a deep interest in the computer world.

His present knowledge of computer technology has been acquired actually through trial and error. He did attend a Regional Occupation Program (ROP) which taught computer programing. Due to his background, he ended up as a teacher's assistant in that program and was instructing other students. His grade average in high school would not be indicative of his overall ability. His grade average was low. He explained this was caused by him being taken out of school several times and traveling in the United States. He has lived in California off and on for many years. He has also lived in Alaska with his parents.

His father is self-employed and owns [redacted]. He cannot remember the exact address, but it is located in the Kearny Mesa area of San Diego. The father has five to six employees. The mother also works with the father. [redacted] advised that his father's name is [redacted] His father changed his name to [redacted] after seeing it mentioned in a science fiction novel. b6 b7C

[redacted] was reminded of a phone call that occurred on October 14, 1983, wherein he had a conversation with the interviewing agent. In that conversation, he had told the interviewing agent that he was in fact [redacted] stated that he was indeed [redacted] He had been reluctant to reveal this fact to the Federal Bureau of Investigation (FBI) b6 b7C

Investigation on 10/14/83 at [redacted] File # SD 196B-1018

by SA [redacted] :rm Date dictated 11/16/83 b6 b7C

SEARCHED INDEXED SERIALIZED FILED DEC 1 - 1983 FBI — ALEXANDRIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

agents who searched his residence on October 13, 1983, pursuant to a search warrant. He thought the purpose of the search concerned another matter involving the family. He briefly described the homicide of an aunt, which had occurred earlier in the year. He advised that he now understood the purpose of the FBI's presence on the preceding day as well as today. He decided to use the name or handle [redacted] after calling in on a "Bulletin Board." One of the other party's using the "Bulletin Board" at the time asked him what his "handle" was. Since he could not or would not use his own true name, he thought of [redacted] He had heard it used before. b6 b7C

He has contacted hundreds of individuals on the telephone lines by using the computer as the father purchased a computer for him approximately nine months ago. The first computer terminal that he had was an Ace 1000. The brand name was Apple. He had another computer before that. That unit was given to [redacted] who resides in [redacted] b6 b7C

His purpose in gaining access to various top communications networks in the United States was to learn more about computers. He simply would access a system, learn as much as he could about it, and then contact the programmers. He frequently talked with programmers regarding the system. Many of the discussions he had with programmers regarding the systems concerned the lack of security.

One of the frequent networks that he accessed was GTE's Telemail System. He recalled one account that utilized the GTE system as that of Raytheon. He also recalled being furnished an administrative password called PROMO. He obtained this from another "hacker" named [redacted] This individual was living in Colorado and frequently used the "Bulletin Board." [redacted] had no idea whether [redacted] was a male or a female. Their communication was conducted on a test loop. Conversations could occur without using any telephone numbers. All that had to happen was to have individuals call in on the access telephone number to the Telemail System. b6 b7C

Access to these telephone lines usually involved dialing the local telephone number for the Telemail System. Once into the system, a series of numbers would be dialed and the systems' "Bulletin Board" would be brought up on a viewing screen. As he mentioned earlier, most of his involvement was with the Raytheon account. He did access a few others. Most of the accounts he accessed were what he called powerless. All an

individual could do in that type of account was to send and receive mail. There was no ability to create or eliminate an account. A message could be added or deleted as wished. On occasions, he did access an administrative account. Once identifying the parameters of that account, he was able to set up accounts of a lower status. With that type of account, one could simply make a private account and furnish it its own access code.

He stated that he thought the "Bulletin Board" with Raytheon was for public use. Anyone could access the system with the proper equipment and read it.

The identities of other "hackers" were discussed with [redacted]. He advised that he does not know [redacted]. He advised that [redacted] b6 b7C The name [redacted] is also known to him as a young lady. He does not know her last name and, as far as he knows, she does not have a home computer.

He denied any deliberate effort to interfere or delete information involved in the computer nets. He had seen comments posted on the "Bulletin Board" indicating that various "hackers" had become bored and had deleted units from whatever communications system they had accessed. He did not admit to doing any of the deletions. He advised that he had not cracked the bank computers, yet. As far as any other computer networks, he has simply been on the network to see what it was all about and then had simply signed off.

He wrote a letter to GTE and discussed the lack of security with the Telemail System. As he had mentioned earlier, Telemail had serious security flaws. This letter was written circa May of 1983. GTE never responded to his letter.

As far as the security of Telemail or any other computer networks, most of the low level accounts within the system have little or no security. Selling of passwords to such accounts is common. By experimentation, many of the accounts can be accessed simply by using one letter passwords. He has heard of a "hacker" or group of "hackers" who make money by selling the passwords to the accounts. In fact, some of these "hackers" have offered to create an account for a fee. They were making money from the Telemail System by creating accounts. [redacted] b6 b7C recalled the group's name as the "time core," or "pirates cave," or "pirates cove."

 b6 b7C

[redacted] advised he sold an RCA terminal modem to a pawn shop for $170.00. The pawn shop is located in the downtown area of San Diego. He could not recall the name of the pawn shop. He advised that since he does not have a driver's license, he was transported by a friend to the pawn shop so as to make the deal. He would not identify his friend during this interview. He advised that he would contact him and obtain the location of the pawn shop so as to confirm the sale of the unit.

[redacted] The inner circle was a group of "hackers" that attempted to form a club. The group never became involved in anything and as far as he knows, they have all broken up. [redacted] Address information as to this individual's whereabouts would be in the materials seized by the FBI. He once acquired an account from [redacted]

b6 b7C

[redacted] was also familiar with ARPANET. He knew this to be a government's system involved in research matters. he was not involved in this system. He knew that several universities were using it. He did not know the access code to get into that system.

b6 b7C

The following description was obtained from interview and observation:

Name:
Sex:
Race:
Date of Birth:
Place of Birth:
Address:

Education:

Occupation:
Hair:
Eyes:
Father's name:

[redacted]

b6 b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription November 2, 1983

[redacted] was telephonically contacted at his residence, [redacted]. He was reminded of a conversation which had occurred between him and the writer on October 14, 1983, at his residence. That discussion had been preceded by an admonishment of his rights. During that discussion, he was questioned as to the location of an RCA Data Terminal, also known as a "modem". b6 b7C

He advised that he had pawned the "modem" at a pawnshop located in the downtown area of San Diego. He had received approximately $170.00 for it. He could not recall the exact location of the pawnshop, and he did not have a receipt showing the transaction. He added that a friend of his had transported him to the downtown area because he did not have a drivers license. He would not furnish the identity of this friend. He would contact his friend and obtain the address of the pawnshop so that the sale of the Data Terminal could be confirmed.

He was now queried as to the results of his inquiry with his friend. He stated he had a correction to make regarding his previous interview. He initially said he had sold the "modem" to a pawnshop when, in fact, he had sold it to his friend. His friend had returned the terminal to him and was quite concerned over the recent publicity concerning the searches that occurred throughout the United States. The friend no longer wished to be involved with him. [redacted] said that he would voluntarily turn the "modem" over to the investigating agent, and that it could be picked up at his residence during the afternoon of October 17, 1983. b6 b7C

At approximately 1:15 P.M., the RCA "modem", Serial Number 001034, Model Number UP3501, along with a small power supply and assorted connecting cables, was picked up at the residence of [redacted] in [redacted]. b6 b7C

He commented at this time that he had been told by friends to seek the assistance of an attorney and discuss the facts regarding his involvement in the illegal entry into the Telenet Computer System. As of yet, he had not retained counsel and queried the writer as to what he should do. He was reminded

Investigation on October 17, 1983 at [redacted] File # SD 196B-1018-35

by SA [redacted] jmj Date dictated October 18, 1983 b6 b7C

SERIALIZED FILED DEC 1 1983 FBI — ALEXANDRIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

23 146

of his previous interview with the writer wherein he had been advised of his rights, including the right to counsel. He was told the decision was his to make. He then asked what he should do in the event the news media contacted him regarding his participation in the computer fraud. He was advised by the writer that any contact or discussion with the media would be left as his prerogative.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/31/83

[redacted], telephone [redacted], was advised of the identity of the interviewing agent and that the interview concerned an investigation involving the penetration of the GTE-Telenet/Telemail Computer Network. [redacted] advised he had information concerning this matter and requested that his identity be protected and that the information furnished be kept confidential. [redacted] furnished the following information:

[redacted]

[redacted]

[redacted]

[redacted]

b6
b7C
b7D

Investigation on 10/13/83 at [redacted] File # SD 196B-1018 -19

by SA [redacted] /jaf Date dictated 10/14/83

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

SERIALIZED FILED
DEC 1 1983
FBI — ALEXANDRIA

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/24/83

[redacted] b6 b7C b7D

telephone [redacted], who was advised of the identity of the interviewing agent and the purpose of the interview, provided the following information:

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

[redacted] b6 b7C b7D

Investigation on 10/17/83 at [redacted] File # SD 196B-1018

by SA [redacted] /cm Date dictated 10/20/83 b6 b7C

SERIALIZED FILED

DEC 1 1983

FBI - ALEXANDRIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

27 150

FD-302 (REV. 3-8-77)

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 9/20/83

[redacted], hereinafter referred to as [redacted] and [redacted] hereinafter referred to as [redacted], were interviewed at the offices of Home Federal Savings and Loan, 12411 Poway Road, Poway, California. They were being interviewed at the request of [redacted] reside at [redacted], telephone [redacted]. The following information was furnished by [redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

Investigation on 9/8/83 at [redacted] File # SD 87D-10472

b6
b7C

by SA [redacted] /mg Date dictated 9/16/83

DEC 1 3 1983

FBI — ALEXANDRIA

1 - 176-B-1018 - Info

34

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

152

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 2/10/84

This is a summary of the activities of [redacted] on GTE Telemail.

[redacted] used the names [redacted] and [redacted] on Telemail. b6 b7C

[redacted] was an illegal user in the following companies: BMW, MARAVEN and UAW.

[redacted] accessed Telemail at least 40 times between July 10, 1983, and October 9, 1983. b6 b7C

Records of [redacted] b7E b6 b7C

[redacted] has admitted to the FBI that he did access the Telemail system without authorization and was using the above-mentioned names. b6 b7C

Investigation on 2/6/84 at Alexandria, Va. File # Alexandria 206A-633

by SA [redacted] :gaj Date dictated 2/6/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

37 160

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 2/10/84

This is a summary of the activities of [redacted] on GTE Telemail. b6 b7C

[redacted] used the name [redacted] on GTE Telemail. He was a member of a group known as the INNERCIRCLE and was an illegal user in the legitimate customer AMERICAN HOSPITAL SUPPLY COMPANY (AHSC). [redacted] left four messages on GTE Telemail between the dates of August 15, 1983, and August 19, 1983. b6 b7C

[redacted] has admitted to the FBI that he used the Telemail services four or five times, but did not think that someone else was being charged for the computer time. [redacted] stated he thought that when someone contacted COMPUSERV or the source, then charges would begin to accumulate. b6 b7C

Investigation on 2/6/84 at Alexandria, Va. File # Alexandria ~~286A~~ 196A-633

by SA [redacted] :gaj Date dictated 2/6/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/30/84

[redacted], telephone number [redacted], was advised of the official identity of the interviewing agent and thereafter provided the following information: b6 b7C

He used the name [redacted] on the Osuny bulletin board during the summer of 1983. While looking at messages on this bulletin board, [redacted] was able to see a private message left for another party on that board. This message was from someone using the name [redacted] and the message stated something to the effect that "you can call me at [redacted] said he called the number once to see if it was a working number and a male answered. [redacted] said he did not say anything, but simply hung up. b6 b7C

[redacted] also said that at an electronics show in New Jersey he met a computer enthusiast whose first name was [redacted] said he uses the name [redacted] on the Telemail system and that he [redacted] would leave a welcome message on Telemail for [redacted]. b6 b7C

[redacted] said he used the Telemail service approximately four or five times and in doing so communicated with [redacted] (who he knew to have a real first name of [redacted] and [redacted]. b6 b7C

[redacted] further stated that he did not know that the messages he was leaving on Telemail were being billed to another company. He thought that somehow this was an electronic connection to a Source account or a Compuserve account and that a person would be billed through Source or Compuserve once you have connected with those computers. b6 b7C

[redacted] also provided the following identifying information:

Date of Birth: [redacted]
Age:
Social Security Account Number: [redacted] b6 b7C

Investigation on 1/25/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 1/26/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~49~~ 172

Height:
Weight:
Eyes:
Hair:

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/10/84

This is a summary of the activity of [redacted] on GTE Telemail. b6 b7C

[redacted] used the names [redacted] and [redacted] on Telemail.

[redacted] was a member of the group known as the PHALSERS and was registered illegally as a user in the following companies: BMW, UAW, MARAVEN, TELENET and AHFS. b6 b7C

[redacted] left six messages on Telemail between July 26, 1983, and August 9, 1983.

A fellow "PHALSER" told the FBI that [redacted] is the same person who uses the name [redacted] on various computer bulletin boards. A list of hackers seized from the residence of [redacted], aka [redacted], contains the listing: [redacted]. This phone number is the unlisted phone number for [redacted], also known as [redacted], also said he saw a message on a computer bulletin board stating that [redacted] could be reached at the number [redacted]. The customer name and address for that unlisted phone number is [redacted]. b6 b7C

[redacted] was contacted at that number and he stated that he is the actual subscriber to that number. [redacted] admits to getting numerous calls for [redacted] at this number, but denies being [redacted] OR [redacted] or using the Telemail system. The personal ID of [redacted] on Telemail was [redacted]. b6 b7C

A fellow PHALSER states that [redacted] works in "some sort of informational job, reading stuff over the radio". [redacted] stated he does volunteer work for the [redacted] b6 b7C

NCIC check on [redacted] revealed three past arrests and one conviction as follows: b6 b7C

Investigation on 2/6/84 at Alexandria, Va. File # Alexandria ~~286A~~ 196A-633 SUB P

by SA [redacted] :gaj Date dictated 2/6/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~51~~ 174

[redacted]

b6
b7C

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/27/84

[redacted], was telephonically contacted and advised of the official identity of the interviewing agent and the purpose of the interview. [redacted] thereafter provided the following information. His date of birth is [redacted], and he is employed as [redacted] has two telephone numbers, [redacted] and [redacted]. Both of these numbers have a customer name and address of [redacted] indicated Ruth Benedict was his mother who is now deceased. b6 b7C

[redacted] stated he has a home computer and a modem and a printer. He runs a home bulletin board known as the "[redacted]". The number to call to contact the computer was [redacted] until approximately July 1, 1983, when he switched the modem number to [redacted]. b6 b7C

[redacted] also has a post office box number that he gives out to computer enthusiasts because he does not want to give out his home address. That is, [redacted]. b6 b7C

During July and August, 1983, [redacted] was setting up his bulletin board to accept incoming calls and requested assistance from a friend of his named [redacted]. According to [redacted] is also employed as [redacted] in a [redacted] home telephone number is [redacted], and according to [redacted] has a computer system, a modem, and a printer. b6 b7C

[redacted] said he does not know who [redacted] or [redacted] are. [redacted] denied any involvement in any illegal intrusions into GTE telemail or any other illegal b6 b7C

SAC P

Investigation on 1/12/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:mbe Date dictated 1/13/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

53 176

activities with his computer system. [redacted] also denied any involvement with the illegal use of the IBM ADS Voice Message System. b6 b7C

[redacted] did, however, state that he has received numerous phone calls at the telephone number [redacted] asking for [redacted]. He said these phone calls began during the summer of 1983, and the most recent was approximately one month ago. b6 b7C

During the summer of 1983, [redacted] remembers getting a phone call from someone who identified himself as [redacted]. This person talked with an apparent nasal condition, doing much coughing and blowing his nose and snorting during the conversation. [redacted] called long distance to [redacted] and asked him for a password for his bulletin board. b6 b7C

[redacted] stated he had had some difficulty with the telephone company during the past few months and that he received an additional number from the Chicago Phone Company and due to an oversight by the phone company, had not been billed for this number for approximately six months. This number, [redacted], is the number he presently uses for his computer, and [redacted] further stated that he eventually had to pay the phone company an additional sum of money for phone calls made over the past six months or so. b6 b7C

[redacted] does some work at the Chicago Library Radio Station reading newspaper articles over the air for the blind. This station is known as "CHRIS," which stands for Chicago Radio Information Systems. The similarity between this acronym "CHRIS" and the first name of [redacted] was commented on by [redacted]. b6 b7C

[redacted] said he did not know and had never heard of the names [redacted], and others. [redacted] said he did have a book of user names and true names concerning his home bulletin board and he may have a list of nationwide home bulletin boards on which he wrote the true names of some computer enthusiasts. [redacted] said that he would be willing to make this information available to the FBI. b6 b7C

FD-517 (12-2-77)

FEDERAL BUREAU OF INVESTIGATION

PROSECUTIVE REPORT OF INVESTIGATION CONCERNING

[redacted] 187

also known as [redacted]

[redacted] also known as [redacted]

[redacted] also known as [redacted]

[redacted] also known as [redacted]

FRAUD BY WIRE; CONSPIRACY

b6
b7C

Copy to: 1 - USA, Alexandria, Va.
(Attn: AUSA [redacted])

b6
b7C

183

FBI/DOJ

AX 196A-633

TABLE OF CONTENTS

AX 196A-633

NAME OF DEFENDANTS:

1. [redacted], described as:

Race
Sex
Date of Birth
Height
Weight
~~Social Security~~ Account Number
Address

[redacted]

[redacted] yrs old

b6
b7C

~~C-1~~

187

AX 196A-633

2. [redacted], described as:

Race
Sex
Date of Birth
Height
Weight
Address

[redacted] yrs old

b6
b7C

C-2

188

AX 196A-633

3. [redacted] described as:

Race
Sex
Date of Birth
Height
Weight
Home Address

[redacted] [redacted] yrs old

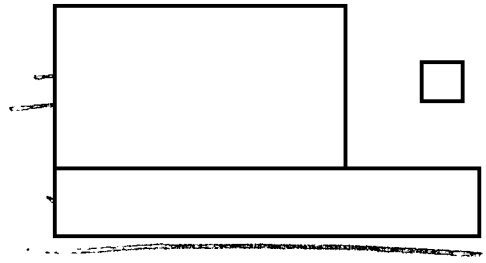
b6
b7C

C-5

AX 196A-633

4. [redacted], described as:

Race
Sex
Date of Birth
Height
Weight
Home Address



[redacted] yrs old

b6
b7C

AX 196A-633

PROSECUTIVE STATUS:

1. On August 30, 1983, the available facts in this matter were presented to Elsie Munsell, United States Attorney, Eastern District of Virginia, who advised she would consider prosecution in this matter.

2. On October 12, 1983, the premises located at [redacted], and [redacted], were searched pursuant to a duly authorized court order and various computer paraphenalia were seized.

b6
b7C

DI

AX 196A-633

WITNESSES:

1. [redacted]
GTE Telemail
8229 Boone Boulevard
Vienna, Virginia
Telephone [redacted]

b6
b7C

Can provide details of GTE Telemail operations, methods of detecting unauthorized users and procedures for obtaining print-outs of customer messages.

2. [redacted]
Special Agent
Federal Bureau of Investigation

b6
b7C

Can supply details of investigation.

3. [redacted]
Special Agent
Federal Bureau of Investigation, Albany

b6
b7C

Can supply details concerning search of [redacted].

4. [redacted]
Special Agent
Federal Bureau of Investigation,
Buffalo, New York

b6
b7C

Can supply details concerning search of [redacted].

E-1

AX 196A-633

EVIDENCE:

RE: [redacted] and [redacted]

1. Summary of messages left on Telemail by [redacted] (originals in possession of [redacted], GTE Telemail). b6 b7C

2. Summary of messages left on Telemail by [redacted] (originals in possession of [redacted]). b6 b7C

3. List of items seized in search of [redacted].

4. Summary of relevant evidence maintained by FBI Alexandria.

5. Summary of trap and trace records received from [redacted] (originals at FBI Alexandria). b7E

6. List of charges attributed to [redacted] and [redacted] (originals with [redacted]). b6 b7C

RE: [redacted] and [redacted] b6 b7C

1. Summary of messages left on Telemail by [redacted] (originals with [redacted]).

2. Summary of evidence retained by FBI Alexandria.

3. Copy of incident report from Nazareth College which implicates [redacted].

4. Summary of nine messages left on Telemail by [redacted] (originals with [redacted]). b6 b7C

5. Copy of trap and trace documents provided by [redacted] (original with FBI Alexandria). b7E

6. List of charges attributed to [redacted], aka [redacted] and [redacted], aka [redacted] (original with [redacted]). b6 b7C

~~F-1~~

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/9/84

The following is a summary of messages left by the illegal user known as [redacted] and [redacted] on GTE Telemail. The date and time of each message is provided, with a synopsis of particularly significant messages included. b6 b7C

1.) August 30, 1983, 6:14 PM (all times Eastern Daylight Time).

2.) August 30, 1983, 9:07 PM.

3.) August 31, 1983, 11:02 AM.

4.) August 31, 1983, 9:02 AM.

5.) August 31, 1983, 3:54 PM.

6.) September 1, 1983, 7:48 AM.

7.) September 1, 1983, 8:04 AM.

8.) August 31, 1983, 7:54 PM.

Note, on September 1, 1983, at 11:03 AM, the illegal user [redacted] received a message from the illegal user [redacted] (aka [redacted]). This message states in part, "He wrote me and told me that if I don't set up accounts a certain way then the company will notice when the bill comes and they will drop the accounts." In this message [redacted] is clearly telling [redacted] (aka [redacted]) that these messages are being placed in the account of a company without that company knowing about it and approving of it and further the company will be billed for the message. b6 b7C

9.) September 2, 1983, 12:10 PM.

10.) September 5, 1983, 7:07 PM.

11.) September 6, 1983, 11:38 AM. In this message [redacted] refers to [redacted] is the true name of [redacted] [redacted] wife. b6 b7C

Investigation on 12/8/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 12/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

F-2

194

12.) September 6, 1983, 3:58 PM.

13.) September 7, 1983, 11:10 AM.

14.) September 7, 1983, 1:59 PM.

15.) September 7, 1983, 2:32 PM.

16.) September 8, 1983, 7:49 AM.

17.) September 8, 1983, 6:12 PM.

18.) September 11, 1983, 6:34 PM.

19.) September 11, 1983, 6:35 PM.

20.) September 12, 1983, 11:27 AM.

21.) September 12, 1983, 1:56 PM. Message refers in part to the purchase of oxygen. This message is in response to a message left on the system by [redacted], stating that the oxygen was ready for pick-up at Rochester Fire and Safety. Investigation by the FBI at Rochester Fire and Safety reveals that [redacted] did, in fact, pick up a respirator on September 12, 1983. b6 b7C

22.) September 13, 1983, 7:33 AM.

23.) September 15, 1983, 9:04 PM. Message states in part "I was unable to log into Telenet, til now. The lines were busy all day. I don't know what all the action was for on Telenet, but it looks like everyone was doing there last minute business reports today."

24.) September 16, 1983, 8:00 AM. Message reads in part "I check the Lincom board this morning, and much to my surprise I found nothing of: use and/or value. I think that you should pass alont (SIC) to the Admin, that we need support here in the field, and the board should contain important information dealing with the everyday usage of this system."

25.) September 18, 1983, 10:01 AM. Message states in part [redacted], from the Okla, sales office has made national news. He was in one of the mag's this month." This statement refers to the fact that [redacted], aka [redacted], was quoted in a national computer magazine in an article concerning computer hacking. b6 b7C

26.) September 18, 1983, 10:21 AM.

27.) September 18, 1983, 4:07 PM. Message refers to [redacted], aka [redacted], is the roommate of [redacted] at Cornell University. b6 b7C

28.) September 19, 1983, 9:32 AM.

29.) September 21, 1983, 7:45 PM.

30.) September 21, 1983, 7:44 PM.

31.) September 23, 1983, 9:03 AM.

32.) September 23, 1983, 5:12 PM.

33.) September 22, 1983, 2:31 PM.

34.) September 23, 1983, 5:18 PM.

35.) September 24, 1983, 5:29 PM.

36.) September 25, 1983, 9:19 AM. This message refers to [redacted], meaning [redacted] wife. b6 b7C

37.) September 26, 1983, 3:55 PM.

38.) September 26, 1983, 1:52 PM.

39.) September 27, 1983, 3:00 PM.

40.) September 27, 1983, 6:27 PM.

41.) September 28, 1983, 11:44 AM.

42.) September 28, 1983, 11:33 AM.

43.) September 28, 1983, 4:39 PM.

44.) September 30, 1983, 8:35 AM.

45.) October 2, 1983, 12:27 PM.

46.) October 2, 1983, 12:23 PM.

47.) October 2, 1983, 3:47 PM. This message again refers to [redacted], meaning [redacted] roommate at Cornell. b6 b7C

48.) October 2, 1983, 3:55 PM. This message states "The A/C you know the number is [redacted]." (Subscriber to number is unknown.) b6 b7C

49.) October 3, 1983, 6:22 PM.

50.) October 3, 1983, 1:13 PM.

51.) October 3, 1983, 4:34 PM.

52.) October 4, 1983, 1:50 PM.

53.) October 5, 1983, 10:24 AM.

54.) October 5, 1983, 10:26 AM.

55.) October 5, 1983, 3:41 PM.

56.) October 6, 1983, 12:39 PM. This message states in part "How about that for balls, giving a story like I did to [redacted]? Well, it would have been nice if it had worked though." This statement refers to the message left by [redacted] on October 5, 1983, at 3:41 PM, wherein he states he talked to [redacted] at American Community and told [redacted] the false story that he [redacted] was doing a story on companies like American Community. [redacted] was attempting to get information about decoders or descramblers for cable t.v. systems. b6 b7C

57.) October 6, 1983, 12:41 PM.

58.) October 6, 1983, 6:12 PM.

59.) October 7, 1983, 8:16 AM.

60.) October 6, 1983, 6:51 PM.

61.) October 6, 1983, 7:40 PM. This message states in part "The cable company there is semi-smart. I will have to work on [redacted] to find out what type of decoder system they are using. I think that I could get the info, but if I don't you can't go wrong with sine wave." b6 b7C

62.) October 7, 1983, 4:22 PM.

63.) October 10, 1983, 4:49 PM.

64.) October 10, 1983, 4:47 PM.

65.) October 11, 1983, 11:01 AM.

66.) October 11, 1983, 1:11 PM.

67.) October 11, 1983, 1:05 PM.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/9/84

The following is a summary of messages left by the illegal user known as [redacted], and [redacted] on GTE Telemail. The date and time of each message is provided, with a synopsis of particularly significant messages included. b6 b7C

1.) August 30, 1983, 7:19 PM (all times Eastern Daylight Time). This message contains the name [redacted] and is signed "Love [redacted] is the true name of [redacted]. She is the wife of [redacted], aka [redacted] and [redacted]. b6 b7C

2.) August 31, 1983, 10:23 AM. This message also contains the true name [redacted]. b6 b7C

3.) August 31, 1983, 10:24 AM.

4.) August 31, 1983, 2:23 PM.

5.) August 31, 1983, 3:38 PM.

6.) September 1, 1983, 10:57 AM. This message is from [redacted] She has now changed her user name from [redacted]. b6 b7C

7.) September 2, 1983, 11:54 AM.

8.) September 5, 1983, 12:05 PM. This message again has the true name [redacted]. b6 b7C

9.) September 6, 1983, 9:16 AM.

10.) September 6, 1983, 9:22 AM.

11.) September 6, 1983, 11:14 AM.

12.) September 6, 1983, 12:43 PM.

13.) September 6, 1983, 1:31 PM.

14.) September 7, 1983, 2:17 PM.

Investigation on 12/8/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 12/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

15.) September 8, 1983, 9:16 AM.

16.) September 8, 1983, 1:44 PM.

17.) September 8, 1983, 1:52 PM.

18.) September 9, 1983, 9:03 AM.

19.) September 12, 1983, 12:32 PM. This message is from [redacted] to [redacted] and is as follows "I do believe that I told you to expect quite a bit higher than you were but I must admit that that is even higher than I thought. Also Roch Fire and Safethy (SIC) called and said that the O2 is ready and the balance due is $164." Investigation by the FBI at a firm called Rochester Fire and Safety indicated that [redacted] did, in fact, have an order for a respirator and that the balance due was $164. [redacted] picked up that respirator on September 12, 1983. b6 b7C

20.) September 12, 1983, 3:24 PM.

21.) September 12, 1983, 3:08 PM.

22.) September 16, 1983, 12:48 PM.

23.) September 17, 1983, 9:55 PM. This message contains the true name [redacted] and is signed Love, [redacted]. b6 b7C

24.) September 18, 1983, 1:21 PM.

25.) September 19, 1983, 10:21 AM. This message asks "How does [redacted] feel about your little discovery (rebooting his system)? If he's anything like [redacted], it is probably a little unsettling." These names refer to [redacted], [redacted] roommate at Cornell, and [redacted], husband. b6 b7C

26.) September 19, 1983, 10:23 AM.

27.) September 19, 1983, 2:31 PM.

28.) September 20, 1983, 10:02 AM.

29.) September 20, 1983, 10:09 AM.

F-8

200

30.) September 20, 1983, 11:38 AM.

31.) September 20, 1983, 3:46 PM.

32.) September 21, 1983, 2:59 PM.

33.) September 22, 1983, 11:13 AM.

34.) September 22, 1983, 2:53 PM.

35.) September 23, 1983, 10:23 AM.

36.) September 23, 1983, 11:33 AM.

37.) September 23, 1983, 2:41 PM.

38.) September 26, 1983, 9:17 AM.

39.) September 26, 1983, 9:17 AM.

40.) September 26, 1983, 9:25 AM.

41.) September 26, 1983, 9:41 AM.

42.) September 26, 1983, 10:51 AM.

43.) September 26, 1983, 12:06 PM.

44.) September 26, 1983, 3:32 PM.

45.) September 26, 1983, 5:48 PM.

46.) September 27, 1983, 4:19 PM.

47.) September 27, 1983, 7:23 PM.

48.) September 27, 1983, 4:11 PM.

49.) September 28, 1983, 10:06 AM. This message is to [redacted] and uses the name [redacted], referring to [redacted] b6 b7C

50.) September 28, 1983, 11:55 AM.

51.) September 29, 1983, 6:27 PM.

52.) September 30, 1983, 8:58 AM.

~~E 9~~

201

53.) October 1, 1983, 3:59 PM. This message is from [redacted] to [redacted] to her husband [redacted]). The message reads in part "Well, I finally got through. I didn't know your name. I had forgotten what you had said it was. You really ought to investigate on that [redacted] user on here. Who knows, with your hacking ability you may come up with something interesting." b6 b7C

54.) October 2, 1983, 1:37 PM.

55.) October 2, 1983, 6:38 PM.

56.) October 3, 1983, 9:44 AM.

57.) September 30, 1983, 8:58 AM.

58.) October 2, 1983, 1:29 PM.

59.) October 2, 1983, 1:42 PM.

60.) October 2, 1983, 6:34 PM.

61.) October 3, 1983, 9:37 AM.

62.) October 3, 1983, 3:26 PM.

63.) October 3, 1983, 3:29 PM.

64.) October 4, 1983, 11:12 AM.

65.) October 4, 1983, 2:42 PM.

66.) October 4, 1983, 11:23 AM.

67.) October 5, 1983, 3:47 PM.

68.) October 6, 1983, 1:16 PM.

69.) October 6, 1983, 1:07 PM.

70.) October 10, 1983, 2:41 PM.

71.) October 10, 1983, 5:54 PM.

72.) October 7, 1983, 3:25 PM.

73.) October 11, 1983, 1:46 PM.

74.) October 11, 1983, 3:08 PM.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/19/83

Pursuant to a search warrant, a search was conducted at [redacted]. The premises were entered at 9:00 a.m. and exited at 10:52 a.m. b6 b7C

The following items were taken from the residence and receipted for:

1. Manilla folder with tapes, computer printouts and miscellaneous items from cabinet in garage - all computer related.

2. Hayes Smart Modern 300, 552094725

3. Radio Shack TRS 80, Model 3, SSAN (SOcial Security Account Number) [redacted] on it. b6 b7C

4. Power source Hayes, lead

5. Two disc drives
   a) Tandon 100-1
   b) Sugart SA-400

6. Printer Gemini 10X 3013024363

7. Flip-N-File Programs

8. Digital timer - Sony 023702

9. Columbia Stereo amplifier

10. SPR-4 - Drake Manuals (two)

10a. Miscellaneous documents from [redacted].

11. Printout paper

b6 b7C

[redacted]

AX 196A-139

Investigation on 10/12/83 at [redacted] ~~Buffalo 196A-529~~

SA [redacted] ; SAA [redacted] and SA [redacted] b6 b7C

by [redacted] JK;kah Date dictated 10/13/83

This document contains neither recommendations nor conclusions of the FBI. It is the property of the F and is loaned to your ag[illegible] and its contents are not to be distributed outside your agency.

~~F-12~~ 204

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 12/7/83

The following is a review of evidence seized pursuant to a duly authorized Federal Search Warrant, executed at the premises known as [redacted], the residence of [redacted]. b6 b7C

The following is a summary of evidence relevant to this investigation:

1) Two yellow cards with the printing, [redacted] b6 b7C

2) A printout with the words, "Computer located at," and six phone numbers listed.

3) A printout with numerous bulletin boards and phone numbers associated with those bulletin boards.

4) A white piece of paper with numerous numbers of unknown meaning on it.

Investigation on 11/15/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] /DF:mb Date dictated 11/16/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~F-13~~ 205

FD-302 (Rev. 3-10-82)

FEDERAL BUREAU OF INVESTIGATION

1 Date of transcription 1/20/84

The floppy discs seized in the search of the residence of [redacted] were examined by [redacted] a computer programmer, and [redacted] stated no information pertaining to GTE Telemail was found. b6 b7C

Investigation on 1/17/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 1/17/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~F-14~~ 206

FEDERAL BUREAU OF INVESTIGATION

1

Date of transcription 1/27/84

The following is a review of [redacted] and trap and trace information received from [redacted] b6 b7C b7E

A review of [redacted] b7E

A review of the trap and trace computer print-outs indicated the following [redacted] b6 b7C b7E

[redacted] b7E

[redacted] b6 b7C b7E

Investigation on 1/19/84 at Alexandria, Va. File # Alexandria 196A-633

by SA [redacted] :gaj Date dictated 1/19/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/31/84

On January 24, 1984, [redacted], GTE-Telemail, provided a copy of the amount of money lost by GTE Telemail from the unauthorized use by the hackers. This document is broken down by user and by company. b6 b7C

Many of the hackers had two or more user names, therefore the following will be a summary of the above document, indicating totals by each user, combining multiple user names (this summary covers the months of July, August and September for each company):

USER	COMPANY	AMOUNT	MONTHS
[redacted]	AHSC	$62.29	July, August, September
	UAW	$31.00	September
[redacted]	Maraven	$16.00	August, September
	Telenet	$108.00	July, August
[redacted]	BMW	$0.29	September
		$127.58	
[redacted]	CBOT	$2.00	September
[redacted]	RADA	$1.00	September
		$3.00	
[redacted]	Maraven	$24.00	August
	Telenet	$325.00	July
	Telenet	$151.00	August

b6 b7C

b6 b7C

b6 b7C

Sub H [redacted]

Investigation on 1/25/84 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted] :sfk Date dictated 1/25/84 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~F-16~~ 208

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/9/84

The following is a summary of messages left by the illegal user [redacted] and [redacted] on GTE Telemail. b6 b7C

The date and time of each message is provided with the synopsis of particularly significant messages included.

1.) August 30, 1983, 12:56 AM (all times Eastern Daylight Time). This message discusses how to set up illegal user accounts.

2.) August 30, 1983, 4:19 PM. This message states "Hi [redacted]. I got our new accounts up. [redacted] will never find these. (I hope) Tell [redacted] that her account is ready [redacted]. See ya. Signed [redacted]." [redacted] refers to [redacted], aka [redacted] is the illegal user name for [redacted] is her password on the Telemail System. b6 b7C

3.) August 30, 1983, 8:20 PM. This message tells [redacted] how to use the Telemail System.

4.) August 30, 1983, 10:54 PM.

5.) August 30, 1983, 8:18 PM.

6.) August 30, 1983, 4:18 PM.

7.) August 31, 1983, 12:56 PM. This message refers to [redacted]. b6 b7C

8.) September 1, 1983, 3:18 PM. This message reads as follows [redacted], I got a list of RADA accounts and yours were there too. So that does not seem to hide them. Also, [redacted] is set up strangely in that you can only use certain configs. Please explain. My accounts are under RADA, even though there are only a few. I frankly think [redacted] is dangerous, since [redacted] does not have a particularly good reputation, and saying [redacted] is run by [redacted] will be sure to get it looked at if anything is looked at. As of now, accounts ([redacted], etc.)" are b6 b7C

Investigation on 12/8/83 at Alexandria, Virginia File # Alexandria 196A-633

by SA [redacted]:gaj Date dictated 12/8/83 b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

under RADA. If you get a list of RADA accounts, you also get some that maybe you created ([redacted], etc.). I have not looked into it but if those are under [redacted] they are also showing up under RADA since [redacted] is a subset of source. Will call you. [redacted]." b6 b7C

9.) September 1, 1983, 4:44 PM. Message reads as follows "[redacted], I don't know what you are trying to find out (i.e. your findings) but the other accounts are: [redacted]. There is nothing wrong with the accounts, but if you find anything, let me know. [redacted] is under [redacted], and [redacted] is under RADA, all others of mine are under RADA. [redacted] P.S. call me when you get in, if busy try again in five. See ya [redacted]." b6 b7C

10.) September 1, 1983, 4:48 PM.

11.) September 1, 1983, 10:14 AM. This message reads in part "Send me mail with the options for the "Admin not noticing." This message refers to continuing attempts to keep the legitimate administrator of an account from knowing there are hackers in his company's account.

12.) September 1, 1983, 8:47 AM. This message refers to the fact that [redacted] as the administrator is going to change the user name of [redacted] to [redacted]. b6 b7C

13.) September 1, 1983, 11:21 AM.

14.) September 1, 1983, 11:03 AM. This message reads as follows "[redacted], as you can see, your name has been changed to its proper name (also, please send mail to me to [redacted]). I finally got it I think. And hopefully [redacted] won't screw us up again. He wrote me and told me that if I don't set up accounts a certain way then the company will notice when the bill comes and they will drop the accounts. I think he is bullshitting me because he wants to have full control of the system. Oh well I told him to tell me what the correct set-up params are so I can do it. Talk to you later [redacted]." b6 b7C

15.) September 1, 1983, 5:19 PM.

16.) September 6, 1983, 8:37 AM.

17.) September 5, 1983, 3:29 PM.

18.) September 5, 1983, 8:24 PM. This message contains the name [redacted]. b6 b7C

19.) September 4, 1983, 11:02 PM.

20.) September 6, 1983, 10:54 AM.

21.) September 5, 1983, 3:27 PM. This message contains the sentence "I just got back (3:19) and [redacted] (my roommate) just walked in." This sentence indicates that [redacted] is the illegal user name for his roommate, [redacted]. b6 b7C

22.) September 6, 1983, 3:41 PM.

23.) September 6, 1983, 6:02 PM.

24.) September 6, 1983, 6:03 PM.

25.) September 6, 1983, 6:04 PM.

26.) September 6, 1983, 6:09 PM.

27.) September 7, 1983, 12:41 PM.

28.) September 7, 1983, 12:50 PM.

29.) September 7, 1983, 4:36 PM.

Note, on September 7, 1983, at 2:14 PM, [redacted] received a message from [redacted]. This message begins Gee, [redacted] I guess there is always a first time. In this message [redacted] uses the true first name for [redacted]. This message also refers to [redacted] meaning [redacted]. b6 b7C

30.) September 8, 1983, 8:44 AM.

31.) September 7, 1983, 11:42 PM.

32.) September 7, 1983, 11:37 PM.

33.) September 8, 1983, 10:52 AM.

34.) September 8, 1983, 10:44 AM. In this message [redacted] uses the name [redacted] referring to [redacted], aka [redacted]. b6 b7C